VOLUME 5:

Information Technology

TABLE OF CONTENTS

VOLUME 5: INFORMATION TECHNOLOGY

a. Technical Environment 1

b. Operating System/Network Software 11

c. System Compatibility 18

d. Network Configuration and Architecture 23

e. Ability to Provide a Secure Electronic Data Interface 32

f. System Downtime and Change Management Process 34

g. IT Personnel Training 39

h. System Data Archive and Retrieval 42

i. System Security and Audit Trail 49

j. Information Systems Data Mapping 58

k. Data Flows and System Edits 76

l. Testing Plan and Data Conversion 94

NARBHA's Management Information Systems Department (MIS) provides a robust, standards-based information systems technical environment that supports and promotes the company's health care mission. MIS has devoted considerable time and attention to ensure that the hardware and software platforms implemented meet the needs of NARBHA and its Service Area Agencies (SAAs) and are state-of-the-art, reliable, scalable, and secure. MIS bases its hardware and software procurement decisions on finding the most efficient tool for the job, compatibility with existing equipment and other network environments, return on investment, product line maturity, and industry research such as trade-specific literature.

NARBHA's technology infrastructure includes a Local Area Network (LAN) and Wide Area Network (WAN). The LAN covers NARBHA's Flagstaff headquarters building and connects all NARBHA users to each other and to the servers (detailed below). For details on the LAN architecture, please refer to Diagram 5.d.1. The WAN covers NARBHA headquarters, (the core site) and 24 SAA locations throughout Northern Arizona. The 24 SAA locations consist of 6 intermediate sites (locations with direct connectivity to NARBHA headquarters) and 18 edge sites (connecting directly to the intermediate sites and, through them, to NARBHA's core site). Private, point-to-point T1 circuits connect video, voice, and data traffic throughout the WAN. The WAN infrastructure, consisting of telecommunications and routing hardware, enables secure and efficient communications to, from, and among NARBHA's SAAs. NARBHA employs multiple servers located at its Flagstaff headquarters to provide various information systems services to its headquarters (via the LAN) as well as to its network of SAAs (via the WAN).

NARBHA's Tribal Area Agencies (TAAs), which represent another major component of NARBHA's provider network, are involved in technical decision-making as well, but are not physically connected to NARBHA's WAN. TAAs maintain a high degree of autonomy by choice, and NARBHA honors that decision. An invitation is always extended to TAA technical staff to attend the monthly collaborative meeting at NARBHA headquarters and they attend periodically, depending on the agenda items.

The hardware, software, and platforms that comprise NARBHA's data infrastructure are detailed below.

NARBHA'S TECHNICAL ENVIRONMENT

Hardware, Software, and Platforms: Servers

NARBHA MIS has chosen Hewlett-Packard (HP), formerly known as Compaq, as its server platform. HP servers provide proven reliability, superior hardware driver support, and superior management tools for servers on a wide variety of network operating system platforms. Additionally, HP servers have historically been on the forefront of redundant component technologies, and employ the hot plug standard (ability to swap out disks, cards, and power supplies without powering down the server) now used by almost every server hardware vendor. NARBHA purchases all server-related hardware in accordance with a three-year life cycle, thus ensuring state-of-the-art speed and reliability as well as continuing ability to expand to accommodate all network needs. NARBHA keeps all server software current through perpetual software maintenance agreements with the vendors. This allows NARBHA to deploy the most current software revisions legally and after they have passed sufficient testing within NARBHA's environment.

NARBHA has seven main servers. Each server's function(s) and hardware and software specifications are described below.

1. SERVER "OK": *Provides* e*Directory root master replica, file services, plug-and-print services, desktop management services, backup services, and one messaging post office database.*

   Hardware

   - *Server:* HP Proliant DL380 G3
   - *Processing:* Two 2.8 Gigahertz (GHz) Intel Pentium 4 Xeon processors
   - *Memory:* 4 Gigabytes (GB) of PC2100 double data rate synchronous dynamic RAM (DDR SDRAM)
   - *Power Supply:* Two hot-swap redundant power supply modules
   - *Disk Storage:* Six 72GB, 15,000 rpm (fastest disk speed on the market) drives configured for RAID 5 (built-in redundancy of data storage through distributed data guarding) and controlled by a high-performance HP Ultra320 Smart Array SCSI controller at 320 Mb/s

- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through dual Gigabit Ethernet Network Interface Controllers
- *Backup:* An external AIT3 auto loading tape storage library, which backs up software on multiple servers nightly

Software

- *Operating System:* Novell NetWare 5.1 with Support Pack 7
- *Messaging platform:* Novell GroupWise 6.5 with Support Pack 1
- *Backup software:* Computer Associates ARCServe 9.01 for NetWare with Disaster Recovery and Open File Agents
- *Virus Protection:* McAfee NetShield 4.61d with nightly automatic updates of new virus patterns
- *Desktop Management Services:* Novell ZENWorks for Desktops 4.1

2. SERVER "WEB1": *Provides secondary Domain Name Services (DNS), Active Directory domain controller, Dynamic Host Configuration Protocol (DHCP) services, subordinate Certificate Authority, secure web-based enterprise messaging interface (throughout the NARBHA/SAA data network), and system logging services(used for auditing security of network hardware). This server is scheduled for replacement this fiscal year as part of NARBHA's three-year life-cycle replacement plan. Current hardware and software are described below.*

Hardware

- *Server:* Compaq Proliant DL380
- *Processing:* Two 1.0GHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB of SDRAM
- *Power Supply:* Three hot-swap redundant power supply modules
- *Disk Storage:* Six 18.2GB, 15,000 rpm hot-pluggable drives configured for RAID 5 (built-in redundancy of data storage through distributed data guarding) and controlled by an HP Ultra3 Smart Array SCSI controller at 160 Mb/s
- *Tape Storage:* HP SuperDLT 100/200GB internal drive
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through a Gigabit Ethernet network interface controller

Software

- *Operating System:* Microsoft Windows 2000 Advanced Server with Service Pack 4
- *Backup Software:* Veritas BackupEXEC for Windows Servers 8.50 Revision 5372 with disaster recovery agent (enables "bare metal" restore capability for maintaining business continuity)
- *Virus Protection:* McAfee VirusScan Enterprise 7.1.0 with automatic updates of new virus patterns occurring nightly
- *System Logging Services:* Kiwi SysLog Daemon 6.1.0
- *Web-based Enterprise Messaging Components:* Novell GroupWise WebAccess servlets for the secure web-based enterprise messaging interface

3. SERVER "SQL": *Provides primary DNS services, Active Directory domain controller, Root Certificate Authority, SQL database services, and secure web-based content distribution services. This server is scheduled for replacement this fiscal year as part of NARBHA's three-year life-cycle replacement plan. Current hardware and software are described below.*

Hardware

- *Server:* Compaq Proliant DL380
- *Processing:* Two 1.0GHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB of SDRAM
- *Power Supply:* Three hot-swap redundant power supply modules
- *Disk Storage:* Four 18.2GB, 15,000rpm hot-pluggable drives configured for RAID 5 (built-in redundancy of data storage through distributed data guarding) and controlled by an HP Ultra3 Smart Array SCSI controller at 160 Mb/s

- *Tape Storage:* A HP SuperDLT 100/200GB internal drive
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through a Gigabit Ethernet network interface controller

Software

- *Operating System:* Microsoft Windows 2000 Advanced Server with Service Pack 4
- *Backup software:* Veritas BackupEXEC for Windows Servers 9.1 Revision 4691 with disaster recovery agent (enables "bare metal" restore capability for maintaining business continuity)
- *Virus Protection:* McAfee VirusScan Enterprise 7.1.0 with automatic updates of new virus patterns occurring nightly
- *SQL Database Services:* Microsoft SQL Server 2000
- *Content Services:* Interactive Information Technology Content Distributor 3.1 (allows secure web-based targeted information distribution through NARBHA's Intranet/Extranet infrastructure)

4. <u>SERVER "NARBHA_OCS":</u> *Provides* e*Directory root master replica, file services, UNIX print services, File Transfer Protocol (FTP) services, eight enterprise messaging post office databases, and enterprise instant messaging throughout the NARBHA/SAA data network. This server is scheduled for replacement this fiscal year as part of NARBHA's three-year life-cycle replacement plan. Current hardware and software are described below.*

Hardware

- *Server:* Compaq Proliant DL380
- *Processing:* Two 1.0GHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB of SDRAM
- *Power Supply:* Three hot-swap redundant power supply modules
- *Disk Storage:* Six 18.2GB, 15,000rpm hot-pluggable drives configured for RAID 5 (built-in redundancy of data storage through distributed data guarding) and controlled by an HP Ultra3 Smart Array SCSI controller at 160 Mb/s
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through a Gigabit Ethernet network interface controller.

Software

- *Operating System:* Novell NetWare 5.1 with Support Pack 5
- *Virus Protection:* McAfee NetShield 4.61d with automatic updates of new virus patterns occurring nightly
- *Messaging Platform:* Novell GroupWise 6.5 with Support Pack 1
- *Enterprise Instant Messaging Platform:* Novell Instant Messenger 1.0 with Support Pack 1

5. <u>SERVER "GWGATE":</u> *Provides enterprise messaging, Simple Message Transfer Protocol (SMTP) gateway services, and web-based enterprise messaging backend processing.*

Hardware

- *Server:* HP Proliant DL360 G2
- *Processing:* Two 2.0GHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB of SDRAM
- *Disk Storage:* Two 18.2GB, 15,000rpm hot-pluggable drives configured for RAID 1 (built-in data redundancy through disk mirroring) and controlled by a Compaq 5302/64 Smart Array SCSI controller at 160 Mb/s
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through dual Gigabit Ethernet network interface controllers

Software

- *Operating System:* Novell NetWare 5.1 with Support Pack 7
- *Virus Protection:* McAfee NetShield 4.61d with automatic updates of new virus patterns occurring nightly
- *Messaging Platform:* Novell GroupWise 6.5 with Support Pack 1
- *SMTP Gateway services:* Novell GroupWise Internet Agent

- *Web-based Enterprise Messaging Components:* Novell GroupWise WebAccess Agent back-end components for the secure web-based enterprise messaging interface

6. SERVER “MAILSVR”: *Provides the primary message transfer agent for enterprise messaging. This server is scheduled for replacement this fiscal year as part of NARBHA’s three-year life-cycle replacement plan. Current hardware and software are described below.*

Hardware

- *Server:* HP Proliant DL360
- *Processing:* Two 1.4GHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB of SDRAM
- *Disk Storage:* Two 18.2GB, 15,000rpm hot-pluggable drives configured for RAID 1 (built-in data redundancy through disk mirroring) and controlled by a Compaq 5302/64 Smart array SCSI controller at 160 Mb/s
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through dual Gigabit Ethernet network interface controllers

Software

- *Operating System:* Novell NetWare 5.1 with Support Pack 7
- *Virus Protection:* McAfee NetShield 4.61d with automatic updates of new virus patterns occurring nightly
- *Messaging Platform:* Novell GroupWise 6.5 with Support Pack 1

7. SERVER “CMHCHOST”: *Provides the platform for NARBHA’s primary business services, the CMHC Management Information Systems (CMHC/MIS) application package and File Transfer Protocol (FTP) services. This server is scheduled for replacement this fiscal year as part of NARBHA’s three-year life-cycle replacement plan. Current hardware and software are described below.*

Hardware

- *Server:* Compaq Proliant ML530
- *Processing:* Two 933MHz Intel Pentium 4 Xeon processors
- *Memory:* 2GB PC2100 DDR SDRAM
- *Power Supply:* Three hot-swap redundant power supply modules
- *Disk storage:* Two drive cages, each with six 18.2GB, 15,000rpm drives configured for RAID 5+1 (highest possible fault tolerance through use of two redundancy methods: distributed data guarding with hot spare). Each drive cage is controlled by an independent channel on a Compaq 5304/128 Smart Array SCSI controller at 160 Mb/s.
- *Network Interface:* Direct connection to the Foundry FastIron 800 Core Gigabit Switch backplane through dual Gigabit Ethernet network interface controllers
- *Tape Storage:* External AME Mammoth2 auto-loading tape storage library, which backs up server software. Due to the critical nature of this host, an additional internal Quantum DLT 20/40 tape backup device is installed for selective or emergency backups.

Software

- *Operating System:* Santa Cruz Operation (SCO) UNIX OpenServer 5.0.6 with Release Supplement B
- *Virus Protection:* Sophos Antivirus for UNIX with updates of new virus patterns occurring after each new release
- *Backup Software:* Cactus Software’s LoneTar 4.1 with Rescue Ranger Disaster Recovery Agent (enables “bare metal” restore capability for maintaining business continuity)

Server Rack: A Compaq Rack 9000 holds all servers at NARBHA headquarters. This server rack provides security, optimal ventilation, power anomaly protection, and redundant power distribution through connection to two uninterruptible power supply units.

LAN Hardware, Software, and Platforms: Desktops and Laptops

MIS has chosen Dell as NARBHA's desktop standard due to its affordability, ease of repair, and excellent service reputation. All desktop and laptop-related hardware is purchased in accordance with a three-year life cycle, while software is kept current through perpetual maintenance agreements with the vendors, allowing for fixed budgeting of software updates and allowing NARBHA to perform thorough stability and compatibility testing before implementing upgrades.

<u>Desktops:</u> NARBHA employs configuration-management best practices throughout the corporation, with each workstation's hardware and software standardized for compatibility and efficiency of support. Mission-specific software is installed on select workstations and licenses are tracked through a software auditing program (Novell ZENWorks Software Inventory) to ensure licensing compliance.

Hardware

- NARBHA has just completed a company-wide hardware migration to the Dell Optiplex GX270 desktop with a 2.8GHz Intel Pentium 4 processor. Each unit has 1.0GB of RAM and a 40GB hard drive. All units are equipped with DVD players and CD recorders, the existing standard for removable media. Ten desktops have not yet reached the end of their three-year life cycle; these are Dell Optiplex GX260 desktops equipped with 1.8GHz Intel Pentium 4 processors. All desktop systems at NARBHA connect to the Ethernet network at Gigabit speeds. Each desktop PC is protected from power anomalies by its own APC BackUPS RS 500VA uninterruptible power supply.

Software

- *Operating System:* NARBHA has just migrated to Microsoft Windows XP Professional with Service Pack 2.
- *Virus Protection:* McAfee VirusScan Enterprise 7.1.0 with automatic updates of new virus patterns occurring nightly
- *Applications:*
    - *Tier 1 applications:* All NARBHA PCs are equipped with the basic tier 1 applications. These are:
        - Microsoft Office XP Professional productivity suite, consisting of Access, Excel, PowerPoint, and Word
        - The WRQ Reflection TCP suite to connect to NARBHA's SCO UNIX host
        - To connect to file and print services, the Novell client for Windows 4.9 with Support Pack 2a.
        - To connect to the e-mail server, the Novell GroupWise Client for Windows 6.5 with Support Pack 1. Select MIS users connect to Windows 2000 Advanced Servers through Microsoft Terminal Services.
    - *Tier 2 applications:* These are employed by users who need to complete specialized tasks. Examples of tier 2 applications are: Adobe Acrobat, Macromedia Dreamweaver, Microsoft MapPoint, Microsoft Project, and Microsoft Visio. Many other internally developed applications are delivered, or "pushed," to an end-user's desktop using Novell ZENWorks for Desktops.

<u>Laptops:</u> NARBHA maintains a laptop pool so that staff who need to travel, attend meetings, or work from home can check out laptops to use while away from headquarters. NARBHA's standard laptop configuration is updated in accordance with a rotating weekly maintenance schedule. All laptops require a secure login for local use as well as connection to the NARBHA system.

Hardware

- The standard laptop in NARBHA's laptop pool is a Dell Latitude D600 with a 1.4GHz Intel Pentium 4 processor. Each unit has 512MB of RAM and a 40GB hard drive. All are equipped with combination DVD players and CD writers (CDRW), the current standard for removable media. Each laptop carrying case is equipped with a modem cable, Ethernet cable, optical mouse, mobile inkjet printer, laminated inventory sheet, and instructions for use.

Software

- *Operating System:* Microsoft Windows XP Professional with Service Pack 2
- *Virus Protection:* McAfee VirusScan Enterprise 7.1.0 with updates occurring upon successful login to the network

- *Applications:* Microsoft Office XP Professional productivity suite, consisting of Access, Excel, PowerPoint, and Word
- *Security:* When a user checks out a laptop and is away from NARBHA's private data network, the user can connect to the Internet and establish a secure and encrypted connection to NARBHA resources by employing the Cisco Universal Client. Once the user authenticates to NARBHA and the connection is secure, the user can connect file and print services through the Novell client for Windows 4.9 with Support Pack 2a. Additionally, each laptop connects remotely to the enterprise messaging server either with the Novell GroupWise Client for Windows 6.5.1 or through an encrypted GroupWise WebAccess program. Each laptop is installed with a ZoneLabs ZoneAlarm personal firewall, SpyBot Search & Destroy anti-spyware software, and Lavasoft Ad-aware anti-adware software.

LAN Hardware

The LAN infrastructure serves NARBHA's 38,000-square-foot Flagstaff headquarters, where each NARBHA employee has a PC on their desk. NARBHA's LAN transfers data among the NARBHA servers and between NARBHA users and servers at extremely high speeds due to its highly efficient network design. This Gigabit Ethernet LAN consists of a single Main Distribution Facility (MDF) and four Intermediate Distribution Facilities (IDFs). Multiple, redundant Gigabit fiber optic trunks connect the MDF to each IDF. A Foundry FastIron 800 Core Gigabit Ethernet Switch provides a single backplane that allows users to connect directly to network resources on the servers. This innovative design bypasses the traditional tiered-switching employed for server connectivity to the greater data network, thus avoiding the data bandwidth bottleneck that is encountered in many data network environments. Another design feature that enhances data transmission speed: Each blade in the FastIron Switch is controlled by its own Application-Specific Integrated Circuit, which allows servers connected to the same blade to interface without adding to data traffic on the backplane. NARBHA's Gigabit-to-the-desktop data network allows users to transfer data to and from their PCs at full Gigabit speed. All new LAN-related hardware is purchased in accordance with a five-year life cycle.

WAN Telecommunications Hardware

Telecommunications hardware consists of a fully redundant DS3 cabinet. The DS3 is a fiber optic line that carries the equivalent of 28 T1 lines. DS3, as opposed to multiple T1s, provides the efficiency of expedited scalability and a significant overall cost savings. The DS3 terminating at NARBHA's Flagstaff headquarters is channelized (divided) into 28 T1 (1.544Mbps) circuits by an Adtran MX2800 M13 multiplexer unit with fully redundant processor card. These T1 circuits carry video, data, and voice signals. Approximately 30 analog phone lines provide emergency voice, fax, and modem access in the unlikely event of a DS3 failure. Currently, a NET Promina 800 ISDN Switch and Frame Relay Access Device provides Frame Relay and ISDN switching services, sending data and video signals to the NARBHA core router and videoconferencing bridge. The Promina and videoconferencing bridge are scheduled for replacement this fiscal year concurrent with a planned video protocol switch from Integrated Services Digital Network (ISDN) to Internet Protocol (H.323, or video over IP). All telecommunications and WAN-related equipment is supported by battery backup and features redundant power supplies. As the WAN is further improved, all new telecommunications hardware will be purchased in accordance with a five-year life cycle.

Three types of traffic flow over the WAN.

- <u>Data</u> traffic is transmitted to a high-end Cisco 7206vxr core router. This device is responsible for providing data routing among NARBHA headquarters, SAA locations, the Internet, and ADHS/DBHS. Access Control Lists (ACLs) implemented on this core router and all other routers in the NARBHA data network provide packet-level security. By employing ACLs, each data packet header is scanned for a specific type of traffic, and is either permitted or denied through the router. Additionally, by utilizing fully private, point-to-point, dedicated T1 lines, NARBHA is able to reduce exposure to breaches in confidentiality and ensure the integrity of the data traffic. This router is scheduled for an upgrade in support of IP-based video services this fiscal year.

- <u>Video</u> traffic is transmitted through a V-Tel SmartLink Model 2020 videoconferencing bridge, which is capable of connecting up to 20 video endpoints simultaneously. The bridge also can "cascade" with other bridges statewide to run extremely large, multi-site videoconferences. NARBHA will replace this videoconferencing bridge this fiscal year with an IP-capable Polycom Accord MGC-100 bridge, which will allow dynamic bandwidth allocation (using as many T1 channels as are required for a given purpose at a given time) and video call compression throughout the NARBHA network, making more efficient use of existing network bandwidth and averting the need to install additional T1 lines. The new bridge also will allow further video network expansion and connection of more video sites simultaneously.

- Voice traffic is transmitted from the MX2800 multiplexer through a single T1 to two Mitel 200 Hybrid PBX telephony switches. These switches are interconnected with a trunk card and provide voice services for the NARBHA headquarters. The Mitel SX-200 PBX telephone system is a modular, flexible, and scalable solution that offers such features as auto attendant, call identification, and paging. Voice mail messages are stored and distributed by an Applied Voice Technology CallXpress voice mail system.

Hardware and Software Support and Maintenance
NARBHA MIS mandates that all information systems equipment be covered under a maintenance agreement for the life cycle of the product.

In addition to vendor-provided service and support, NARBHA MIS is staffed with specialized skill sets to resolve many of the issues that arise. For example, the WAN Manager is capable of resolving WAN connectivity issues and carrying out WAN hardware troubleshooting. The Network Administrator provides on-site support for servers, printers, print servers, LAN-related hardware, and complex LAN connectivity issues. The LAN Specialist provides desktop repair expertise and is equipped to resolve basic network connectivity issues. The Telemedicine Technical Specialist troubleshoots videoconferencing bridge and endpoint equipment.

- Desktops, laptops, and server hardware are all covered under three-year maintenance contracts that provide replacement parts and problem resolution with either telephone support or, in a worst-case scenario, an on-site technician to troubleshoot a complex hardware-related issue. Dell and HP are the vendors for these contracts, responding to desktop, laptop, and server support requests eight hours per day, five days per week. Replacement hardware is shipped for delivery by the next business day.

- Printing hardware support is provided through HP, the standard manufacturer of all NARBHA printers. HP will respond to printer support requests eight hours per day, five days per week. Replacement printer hardware is shipped for delivery by the next business day. Additionally, on-site technical assistance and bi-annual preventive maintenance is performed by a local HP-authorized repair service, The CyberPROs.

- LAN and WAN hardware are covered under five-year contracts, as that is the expected life cycle of the equipment. Dell and Cisco respond to LAN and WAN hardware support requests 24 hours per day, seven days per week. Replacement LAN and WAN hardware is shipped for delivery by the next business day, while select spare equipment such as Gigabit Switches are maintained at NARBHA headquarters.

- Telecommunications hardware support is provided by NARBHA’s telecommunications provider, Qwest Communications. Support is provided contractually for the life of the service, including NARBHA’s DS3. The scope of support includes Qwest’s telecommunications infrastructure and NARBHA’s customer premise equipment. The contract requires availability for assistance eight hours per day, five days per week, and replacement hardware within four hours. Qwest also is NARBHA’s Internet Service Provider (ISP) and provides the same level of support for two Internet T1 connections and the corresponding IP-based services.

- Videoconferencing hardware support is provided by Net.com for the Promina 800 ISDN/Frame Relay switch and Wire One for the videoconferencing bridge and endpoint equipment. Both contracts are 24 hours per day, 7 days per week, with replacement parts shipped for delivery next business day, and are renewed annually.

- Voice hardware is supported by a local authorized reseller of Mitel products, Teledigit. This company has demonstrated superior customer service over years of service to NARBHA, and is responsible for the installation of NARBHA’s Mitel SX-200 switch, the Applied Voice Technology CallXpress voice mail system, and all Mitel Superset 4150 voice handsets. Teledigit also is NARBHA’s contractor of choice for internal wiring for voice, video, and data services.

- Software maintenance is purchased in accordance with NARBHA’s annual budget cycle, to ensure that the latest version of the software is available. For instance, all Microsoft software is purchased along with Software

Assurance and renewed bi-annually. Novell software is purchased using a Volume License Agreement that is renewed annually. SCO UNIX software maintenance is also renewed annually. All software is supported by its respective vendors through paid technical support calls. A fixed number of technical support calls for each software vendor is included in the annual budget. Subsequently, an open purchase order is pre-approved in order to expedite software problem resolution.

FACILITY: ENVIRONMENTAL AND PHYSICAL SECURITY SAFEGUARDS

All information systems hardware at the Flagstaff NARBHA headquarters is physically secured by employing a layered defense model, meaning security measures increase as one enters deeper into the building.

Starting with the perimeter and building grounds, landscaping is performed so that branches of trees are trimmed to be at least six feet from the ground and bushes are groomed to grow less than two feet tall. Structural barriers allow only foot-traffic entry into the building. Lighting on the outside of the premises automatically illuminates outside areas, beginning at dusk each evening.

The building itself is armed with an alarm system. Employees enter the building using a Simplex card key lock system with tiered access control within different parts of the building. Successful entry is logged to a database within the server-based card key lock system. The database shows an alarm if any keyed door is left open for more than 20 seconds.

Only one exterior door is unlocked during business hours. This door enters into the receptionist area, which is always staffed during business hours. Entrance from the reception area to the rest of the building is by key card only. All visitors are required to sign in and out, must wear numbered visitor badges, and must be escorted at all times by a NARBHA staff member, according to NARBHA Internal Policy 1504, Security Management. In addition, NARBHA staff members are required to wear their picture IDs at all times. All other exterior doorways are dependent on a valid card key to enter. The only windows in the building that can be opened are located on the second floor. For safety purposes, local law enforcement members have been familiarized with the physical layout of the building, while six hand-held radios are routinely monitored from strategic locations within the building to ensure immediate response in the event of emergences. Additionally, fire prevention, detection, and suppression safeguards protect NARBHA employees, visitors, and physical assets.

NARBHA’s secure data center is located at the core of the corporate building and requires a Simplex key card with specific permissions to enter (see Diagram 5.a.1 below). Only select MIS, Telemedicine, and Security staff have access to the data center. The data center has its own air-conditioning units. There are two backup air conditioning units in case of a failure of the main DataAire unit, which services both the temperature and humidity requirements of the data center. The data center also features a false floor, independent electrical facilities, and an Ansul Inergen waterless fire suppression system. Inergen suppressive gas consists of a mixture of nitrogen, argon, and carbon dioxide that will not harm electronic components within the data center. All components of the data center adhere to the ANSI/TIA/EIA-569-A Standard for Telecommunications Pathways and Spaces. The data center is populated with mission-critical telecommunications, data, video, and voice equipment. All equipment is connected to uninterruptible power supplies that provide “clean” power and protect against complete or partial power system failures.

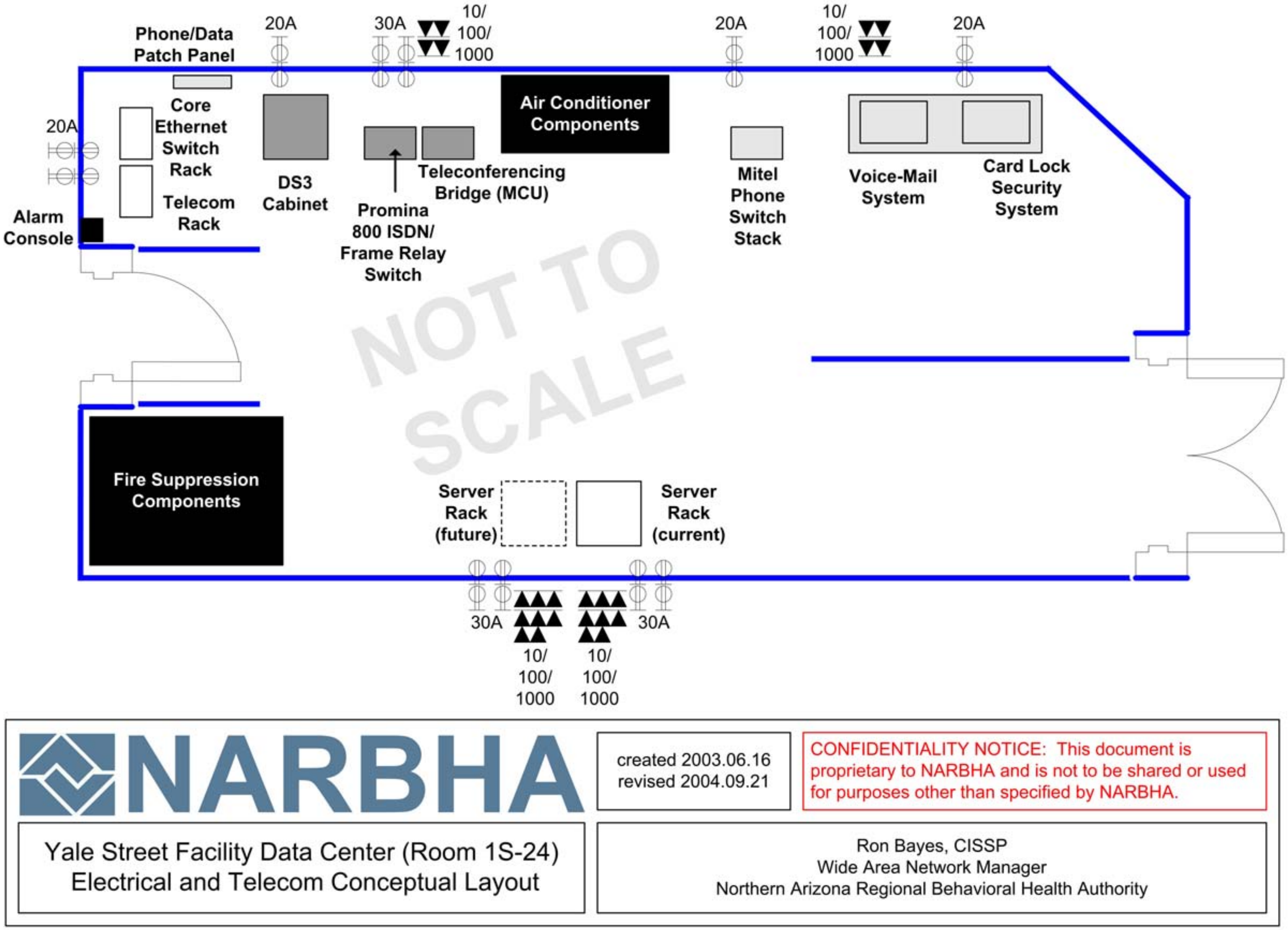
Temperature, humidity, and dew point in the data center are monitored by Ethernet-enabled Newport iServer MicroServer (Firmware 2.1) sensors. These devices are located in each of the Intermediate Distribution Facilities as well as the Main Distribution Facility in the data center. Sampling every 20 seconds allows for web-based charting to determine trends. e-mail alarms notify data network professionals any time thresholds are exceeded.

All information systems equipment or hardware is tagged with a NARBHA Property Control Tag within one month of deployment. Property control logs are maintained by the Business Manager and are inventoried annually for accuracy (NARBHA internal Policy 2101-Physical Control of Assets). This process provides accountability of all NARBHA resources, particularly some of the most valuable resources: those used for information systems.

CONCLUSION

NARBHA maintains a carefully planned, secure, robust, scalable, state-of-the-art information systems technical environment, which readily accommodates all data storage, retrieval, and transmission needs of NARBHA and its SAAs, as well as all e-mail, Internet access, and videoconferencing traffic requirements. The three and five-year life-cycle hardware replacements and regular software updates ensure that the technical environment is consistently able to host and handle ever-increasing data and communications needs, while redundant storage systems and tape backups ensure the safety and integrity of data at all times. NARBHA remains mindful of defense-in-depth security from user education and policies designed to protect individual corporate PCs to sophisticated firewalling at the perimeter of the WAN.

Diagram 5.a.1: NARBHA's Data Center



NARBHA's Management Information Systems Department (MIS) is engaged in all facets of the managed behavioral health care business. NARBHA MIS utilizes integrated technologies not only to support but also to enhance the delivery and management of behavioral health care throughout Northern Arizona.

Operating System and Network Software

MIS bases operating system and network software implementation decisions on finding the most efficient tool for the job, compatibility, return on investment, product line maturity, and industry research such as trade-specific literature.

NARBHA MIS utilizes a mixed network software environment, employing best-in-class solutions to suit business objectives. The standard for network file and print services is Novell NetWare, due to its historically stellar reputation for reliability, file delivery performance, and ability to establish and administrate security all the way down to file level. NetWare is also tightly integrated with *e*Directory, one of the most mature and sophisticated Directory Services on the market. Novell *e*Directory is a distributed directory database that adds efficiency to information services with single authentication, providing users with simultaneous access control to a variety of data network resources. The *e*Directory database is fully replicated among multiple servers at NARBHA headquarters and multiple Service Area Agency (SAA) sites. Novell Netware is the operating system for NARBHA's in-house, custom programmed applications.

NARBHA's primary business application, the CMHC/MIS system, runs on the Santa Cruz Operation UNIX OpenServer 5.0.6 with Release Supplement B operating system on a Compaq Proliant ML530 server, discussed in detail in Volume 5.a.

Programming Language Used for Developing Software

NARBHA's programming environment is a dual structure made up of: 1) a software package purchased from CMHC Systems of Dublin, Ohio, to support the managed care organization and administrative aspects of NARBHA's business; and 2) a mix of custom applications developed and supported in-house to help NARBHA and its SAAs and Tribal Area Agencies (TAAs) meet ADHS/DBHS data submission requirements and to provide customized reporting and data capture processes for NARBHA staff.

<u>Managed Care Organization Programs/Applications Development</u>

NARBHA uses the CMHC/MIS software package to support its managed care organization applications. This software is developed and marketed by CMHC Systems, an industry leader in developing software products for human services organizations since 1978. While NARBHA MIS programmers do not use a programming language to make changes to the actual source code of CMHC/MIS, the software package comes with a robust set of development tools that allow NARBHA system administrator(s) to customize the software extensively through:

- Creation/maintenance of data elements as necessary with the ability to tie those elements to validation rules
- Creation/maintenance of validation rules
- Creation/maintenance of new data capture forms that can be created, amended, and linked together as necessary
- Exports of data from the systems based on specific selection criteria, either pre-defined or interactive
- Imports of data into the systems based on specific criteria, either pre-defined or interactive
- Establishment of access to these functions based on the role established for the end-user
- Creation of reports as necessary through the system
- Creation/maintenance of Uscript-based programs to manage information in the system

While only a system administrator can perform these functions, any end-user with the appropriate access rights can use what the system administrator creates.

The CMHC/MIS system has two major components, each of which performs a specific business function. These are the CMHC Managed Care Organization component (CMHC-MCO) and the CMHC-Accounting component.

NARBHA implemented the CMHC-MCO system to manage information for the following business functions and creation and receipt of the Health Insurance Portability and Accountability Act (HIPAA) standard data transactions for ADHS/DBHS.

- <u>Enrollment/Closures Information</u> is submitted to NARBHA through the HIPAA 834/Enrollment transactions and is incorporated into the CMHC-MCO system after being validated by the Visual FoxPro Collection and Scanner

Program/Edit Reporting (CASPER) program to ensure the information is correct and consistent. The HIPAA/834 adheres to federal standards and ADHS/DBHS specifications. Data are submitted electronically by the SAAs and processed daily. Data for the TAAs are submitted manually and entered at NARBHA into local systems, and later merged into the electronic data submission process the SAAs use.

- Eligibility/Demographic Information is submitted through the NARBHA Companion data set, which contains ADHS demographic data as well as ancillary information required for internal processes. Data are incorporated into the CMHC-MCO system after being validated by the Visual FoxPro CASPER program at NARBHA. Data are submitted electronically by the SAAs and processed daily. Data for the TAAs are submitted manually and entered at NARBHA into local systems, and later merged into the electronic data submission process the SAAs use.

- Contract Information on contracted services for all NARBHA providers is used in the claims adjudication process. This information includes basic provider information, service level data with reimbursement rates, begin/end dates, and permissible service code modifiers that provide additional information on the service and its delivery method.

- Service Authorizations are required for payment of any covered services delivered through a provider identified as a fee-for-service or single-case-agreement (cash payment) provider, as differentiated from a capitated/encounter-based provider such as the SAAs/TAAs. Service Authorization requests are submitted by appropriate staff at the SAA/TAA to NARBHA and are entered into the CMHC-MCO for use in the claims adjudication process.

- Claims Adjudication/Payments is the process where NARBHA accepts behavioral health service claims and processes them against enrollment, contract, and service authorization information to determine whether a claim is to be paid or not. Some specifics in this function are:

  - Claim submission
    - Claim submissions can be in an electronic format submitted from a remote data system.
    - Manual claims can be submitted for data entry at NARBHA.
    - Providers can, with authorization and training, enter their own claims.

  - Adjudication process
    - A standard software package set of adjudication rules is processed against claim data based on standard claims rules.
    - Additional adjudication rules, created by NARHBA systems administrators, are processed against claim data based on Covered Services Rules, ADHS requirements, and NARBHA internal needs.

  - HIPAA Complaint Claims Submission
    - HIPAA 837/Institutional Claims are created after the claims run is completed using CMHC-MCO standard processes, then submitted to ADHS/DBHS.
    - HIPAA 837/Professional Claims are created after the claims run is completed using CMHC-MCO standard processes, then submitted to ADHS/DBHS.

NARBHA uses the CMHC-Accounting system to support many of its accounting functions. CMHC-Accounting also allows a great deal of flexibility in modifying these functions.

- Accounts Payable handles purchase orders, accounts payable invoices, disbursement checks, check reconciliation, and related reporting. The accounting information is integrated with the general ledger function, eliminating the need to export data between systems.

- Payroll computes employee wages, calculates taxes, withholds deductions, figures net pay amounts, and produces paychecks. The payroll system also is integrated with other accounting functions.

- General Ledger functions provide reporting of asset, liability, revenue, expense, and statistical amounts for actual and budget accounts.

Custom Programs/Applications Development

NARBHA's MIS department uses Microsoft Visual FoxPro, Version 7.0, to develop many of its custom applications. Visual FoxPro has been the software development tool of choice at NARBHA since 1993 because it creates stand-alone programs that can be distributed to and run by the SAAs without their having to own their own copy of Visual FoxPro. In addition, the newer versions are object-oriented and thus efficient. As newer versions of FoxPro have been released, MIS programmers have converted essential applications into the new release, preserving the functionality of custom applications. Many of these custom applications have proved so useful to NARBHA that MIS has created SAA/TAA versions and distributed them free of charge to the SAAs/TAAs. Some of the critical applications developed by MIS and in use at this time are:

- CASPER: Used to validate enrollment, eligibility, and demographic information submitted by SAAs/TAAs to NARBHA. The validation takes place at the SAA/TAA level prior to transmission to NARBHA and allows for timely review/correction of errors by SAAs/TAAs.

- Demographic Upload: Used to prepare data extracted from NARBHA's Managed Care Organization (MCO) databases in CMHC and transmit the data to ADHS/DBHS.

- Intelligent Global Gathering Information (IGGI): Used originally to allow internal NARBHA staff to inquire into enrollment and eligibility information for NARBHA members only; now includes all members statewide. IGGI is now available to all SAAs/TAAs.

- Client Information Systems (CIS) Downloads: Used to transfer member information from the ADHS data systems to NARBHA, add it to internal systems at NARBHA, and prepare control reports on accepted and incorrect data. These data include encounters, enrollment, closure, demographic, provider, Arizona Health Care Cost Containment System (AHCCCS) eligibility, Statewide Roster, and third party liability.

- Pharmaceutical Card Systems (PCS) Monthly Update: Used to manage the medication information NARBHA receives from its Pharmacy Benefits Management firm, CaremarkPCS, to balance that electronic information against payments made to CaremarkPCS, create data files to submit to ADHS/DBHS, receive accepted and incorrect data back from ADHS/DBHS, and prepare control reports on accepted and incorrect data.

- Encounter Phase II: Used to prepare reporting files from individual claim level that can be used later to prepare reports, databases, and spreadsheets used by NARBHA and its SAAs/TAAs to track financial management information.

- ERC400/ERC500 Encounter Reports: Used to prepare reports for management at NARBHA and the SAAs/TAAs. Reports are archived, distributed, and printed as necessary.

- Institutions for Mental Disease (IMD) Tracking: Used to track members in IMD facilities and to track their AHCCCS eligibility.

- Child Protective Services (CPS) 24-Hour Response: Used to track CPS reports to NARBHA as children are removed from their home and need assessment.

- Correctional Officer/Offender Liaison (COOL): Used to track members with a substance abuse problem who have recently been released from jail, and to track their service delivery treatment status.

- AHCCCS Provider/Reference File Imports: Used to import AHCCCS provider information, reference files, and prepare reports.

- Capitation File Imports: Used to import the "At Risk" data sets to prepare summary data on penetration for the NARBHA area and to extract information on Comprehensive Medical and Dental Plan eligibility for internal use.

- Withholding: Used to import claim level data that support the ADHS/DBHS withhold process.

MIS also uses Visual FoxPro extensively for preparation of data that are imported into or exported from NARBHA's MCO databases in CMHC for use elsewhere.

While NARBHA has used the Visual FoxPro development tool for over a decade, emerging technologies require that applications be web-based. Many of the applications defined above such as CPS 24-Hour Response, IMD Tracking, CASPER, and IGGI are designed to function on a central file server located at the NARBHA or SAA main site and be available to any staff that have the appropriate rights to use them.

To maximize the user-friendliness and usefulness of its custom-developed applications, MIS has begun the process of integrating the Microsoft Visual Studio .NET technologies into its technology environment, which will allow MIS staff to develop future applications and upgrade current applications as web-enabled, meaning they will be able to function as a web page in NARBHA's Intranet/Extranet environment. NARBHA's Intranet/Extranet environment is currently under development, with MIS using Content Distributor to assign protections to various levels of the NARBHA website at www.narbha.com, so various groups of users have access privileges and see only information that is specifically targeted to them when they log on to the website. Thus, any user in the outside world can see basic introductory corporate information about NARBHA. Outside stakeholders, SAAs/TAAs, NARBHA staff, and other identified groups within the NARBHA system will be assigned special permissions to access only the information that is necessary or relevant to them. For instance, NARBHA department members can share files and SAAs can check the status of claims. This system will allow NARBHA to disseminate information immediately and consistently to every appropriate group. In this new environment, it is critical that all information be protected against inadvertent or malicious disclosure; ensuring this protection is an integral part of the Intranet/Extranet development.

Operating System Updates and Service Pack Deployment

Over the last few years, NARBHA MIS has tested various methods of deploying operating system updates, service packs, and security patches. The Information Technology industry defines the deployment of these types of updates as "patch management." MIS recently chose a patch management solution from Shavlik, based on its track record as the principal developer for the Microsoft Baseline Security Analyzer and the Microsoft System Update Service (SUS) feature pack. NARBHA's patch management solution for user workstations consists of two components called Shavlik HFNetChkPro and Shavlik Security Agent. The HFNetChkPro component resides on a Windows 2000 Server and communicates with workstations on the data network through the Windows client-based Shavlik Security Agent. The noteworthy feature of the Shavlik solution is that it does not require the "File and Print Sharing" service to enable patch application, as many other popular patch management products do. This feature ensures that desktop security is not potentially compromised through unnecessarily enabling the "File and Print Sharing" service. As part of its service to its customer base, Shavlik tests patches and updates fully before it releases them for use. In addition, the MIS data networking team thoroughly tests security updates and service packs prior to wide-scale deployment to ensure compatibility with NARBHA's software environment.

Among NARBHA PCs company-wide, desktop patch revisions are inventoried through their respective Shavlik agent components, which are installed on each PC. Once a patch has been tested, it is deployed to all available desktops throughout the LAN. Minor patches are deployed seamlessly and invisibly to end-user PCs with very little performance degradation, due to Gigabit Ethernet access speeds on NARBHA's LAN. For larger service packs, MIS notifies users via e-mail not to reboot or power off their systems so that patches can be applied overnight. MIS staff collect patch deployment results through the secure web-based interface and reschedule any patch deployments that failed due to PC unavailability or interruption. Server operating system updates and service packs are handled much the same way, with the exception that the larger patches are deployed after normal business hours. This ensures that any outages do not effect day-to-day business operations.

Scheduling of patch deployment depends on the frequency and severity of the patch. Major software vendors do not adhere to schedules in their releases of security patches, so MIS evaluates each deployment on a case-by-case basis. MIS does, however, schedule deployment of larger service packs after careful evaluation of their merit and their impact on the data network. If MIS deems the deployment to be of great value, then MIS staff communicate with end-users via e-mail as to when the patch deployment will occur. Bandwidth on the LAN is virtually unaffected by updates or service pack deployments.

Ability to Purchase Source Code to Customize the Software

NARBHA MIS uses Microsoft Visual FoxPro Version 7.0 to develop many applications. This development tool itself is available for purchase through numerous software resellers. The programs developed using FoxPro are owned by NARBHA; NARBHA has full rights to make any necessary changes to satisfy its business needs and to distribute these programs as it sees fit.

In using CMHC/MIS, NARBHA works closely with CMHC Systems through development committees, regional and national conferences, and direct meetings with CMHC development staff to define enhancements or refinements that NARBHA feels are necessary to the functioning of the CMHC system for NARBHA's environment. Typically these enhancements or refinements are accomplished under the annual support contracts NARBHA has in place with CMHC Systems, but in some instances NARBHA contracts with CMHC Systems to have CMHC staff make specific changes using the COBOL programming language.

To protect NARBHA's investment in the CMHC software, as well as its own business functionality, NARBHA has entered into a source code escrow agreement with CMHC Systems through the law firm of William E. Morse, Esq., of Dublin, Ohio, acting as escrow agent. Under this agreement, the escrow agent, William E. Morse, Esq., will:

- Hold electronic copies of the source code for the CMHC/MIS system(s) in a manner that is available to NARBHA in the event of a failure of CMHC Systems.

- Receive updated source code for CMHC/MIS to ensure that the escrow agent has current versions of the CMHC/MIS sufficient to re-create the systems in the event of a failure of CMHC Systems.

- Commit to release this source code to NARBHA in the event of:
  - Request by CMHC Systems to release the source code to NARBHA
  - Cessation of CMHC Systems to conduct normal day-to-day business operations (business failure, bankruptcy, or voluntary liquidation by directors/stockholders)
  - Default by CMHC Systems as proved by a judgment made by a court of law or an arbitration decision that CMHC Systems has breached the terms and conditions of the License Agreement in an action wherein NARBHA has sought as a remedy a copy of the source code

Through the escrow agreement, NARBHA has protected its functionality by ensuring an ongoing ability to upgrade, maintain, and use its primary business application, even if CMHC Systems were to cease operations. This agreement includes all specialized enhancements that NARBHA has purchased. In the event that NARBHA takes possession of the source code, NARBHA would have the right to change the source code to modify system functionality to meet the changing requirements of NARBHA and ADHS/DBHS.

Policy and Procedure on Software Upgrades

CMHC System(s)

Because the CMHC system is the central repository for all member and claim level data, it is imperative that the software be kept current, so when upgrades are anticipated these upgrades are approached in as formal a manner as possible. To that end NARBHA has established policies governing these upgrades and procedures to follow. A major component of NARBHA's upgrade process is that, due to the integrated structure of the CMHC system, NARBHA has to remain current with all upgrades and patches. A second component is that NARBHA applies upgrades and patches on a weekly basis. CMHC releases upgrades and patches at the start of every week.

It is the policy of NARBHA that the CMHC system will stay current with all patches released. The procedure(s) encompassed within this policy are as follows:

- NARBHA's CMHC Programmer/Analyst or designee logs into the CMHC Systems Bulletin Board every Tuesday morning to see if patches are available and, if they are, downloads patches to a temporary file on its UNIX server. State patches that are not specific to Arizona are ignored.

- NARBHA's CMHC Programmer/Analyst or designee e-mails the patch log to all programmers and parties affected by the patch release. Any concerns are addressed before close of business on Wednesday.

- The CMHC Programmer/Analyst or designee in charge of the patch load is responsible for reading the log and determining functions that will be affected by patch deployment. This programmer also verifies that any changes to functionality will have not have an impact on productivity. If an impact on productivity could occur, the programmer discusses the load of the patch with other programming staff.

- Before close of business each Wednesday it is the responsibility of the CMHC Programmer/Analyst or designee to e-mail NARBHA users that the CMHC system will be unavailable due to patch application on Thursday morning before the start of business (8 a.m.).

- The CMHC Programmer/Analyst or designee records verification of successful CMHC backup before applying the patch to the system one hour before the opening of business on Thursday. If backup failed, the patch is not applied to the system and notification is sent to programmers and affected parties. The application of the patch is then rescheduled.

- The CMHC Programmer/Analyst or designee verifies and documents the successful application of the patch.

- In the event of an unsuccessful application of a patch, the CMHC system is restored to its original state from backup media. Programmers and affected parties are notified of the patch failure. The CMHC Programmer/Analyst or designee in charge of applying the patch contacts the vendor. Appropriate steps are taken by NARBHA and the vendor to resolve the issue(s). Until the issue(s) have been resolved, no patches are applied to the system

The above process is predicated on the upgrade or patch taking no longer than one hour, thus allowing patch application during the work week. With major upgrades, or upgrades that are expected to take appreciably longer than the one hour set aside for this process, the CMHC Programmer/Analyst will take the same steps but will schedule them for a weekend or for evening hours.

Personal Computers/Laptops

As noted above in the section “Operating System Updates and Service Pack Deployment,” NARBHA exercises extreme care in changing and upgrading operating systems and productivity software on these systems. NARBHA has established a series of policies and procedures to govern these processes as follows.

- Software upgrades are researched on Internet message boards, through trade magazines, and with vendor release information prior to consideration for use within NARBHA.

- All software upgrades must be equipped with a de-install or “roll back” capability.

- Software upgrades are tested in a non-mission-critical environment first. This is usually a test personal computer or personal computer in a non-mission critical area.

- Prospective upgrades are tested for a period of at least one week prior to company-wide deployment. Testing is performed by MIS department staff or by other NARBHA staff identified as having expertise in the product to be deployed.

- After deployment the affected systems and software are scrutinized for potential problems.

- Newly identified problems are given immediate attention and the upgrade deployment is halted until the issues are resolved.

- If the upgrade proves to be problematic, a short amount of time is allocated to research the problem to determine if the deployment can be continued. If there is no immediate problem resolution, the upgrade is “rolled back” to the previous version of software in use.

Servers

NARBHA exercises extreme care in changing and upgrading the operating systems running on its core systems/servers, and has established a series of policies and procedures to govern these processes as follows.

- Network Operating Systems (NOS) and/or server-level software upgrades are researched on Internet message boards, through trade magazines, and with vendor release information prior to consideration for use within NARBHA.

- Prior to any upgrade to NOS and/or server-level software, the systems backups are verified to ensure NARBHA will have the ability to de-install or “roll back” the upgrade.

- Wherever possible, NOS/software upgrades are tested on non-mission-critical servers before deployment to mission-critical servers.

- Prospective upgrades are tested for a period of at least one week and as long as deemed necessary by the Wide Area Network (WAN) Manager and/or the Local Area Network (LAN) Manager.

- After deployment the NOS or software is monitored by the WAN Manager and/or the LAN Manager daily to ensure that there are no problems.

- If the NOS or software upgrade proves to be problematic, a short amount of time is allocated to research the problem to determine if the upgrade can remain in place. If there is no immediate problem resolution, the NOS or software upgrade is removed and the server is “rolled back” to the previous version of NOS or software.

NARBHA contracts with nine Service Area Agencies/Tribal Area Agencies (SAAs/TAAs) to serve as the backbone of its provider network. Each SAA/TAA is responsible for providing a comprehensive array of behavioral health services in its sub-region. Fee-for-service (FFS) providers complement the SAAs/TAAs by providing member access to specialty services best provided by niche agencies or services that are not cost-effective in sparsely populated areas. Single case agreement (SCA) providers are used to temporarily expand the NARBHA network when necessary to meet member needs.

NARBHA maintains a lengthy history of computer system compatibility with its SAAs, which provide 94.7% of all service to NARBHA members based on claims/encounter volume. All seven SAAs are connected to the NARBHA Wide Area Network (WAN). There is consistency within NARBHA's entire WAN, from the physical information systems equipment that interconnects various sites within NARBHA's five-county, 62,000-square-mile geographic service area (GSA) to the desktop applications that are used by approximately 1,300 employees of NARBHA and its SAAs. This standardization ensures that NARBHA's Management Information Systems (MIS) Department can efficiently provide information systems support across the network while minimizing the impact on available MIS resources.

When planning for implementation of new systems or changes in existing systems or processes, NARBHA MIS regularly collaborates with the SAAs regarding the technical direction that they have jointly chosen. Input from technical staff at the SAA locations provides a clear understanding of the needs and complexities faced by individual sites. NARBHA MIS makes all major technical decisions with prior input from with key SAA technical staff to gain a full understanding of the potential issues they will face and to create awareness of the importance of the implementation or change. NARBHA MIS meets with SAA technical staff on a monthly basis to stay current with one another and address any issues that arise. This collaboration provides a uniform approach to resolving technical challenges and provides all SAAs an opportunity to be heard and to discuss any concerns.

NARBHA's TAAs are involved in technical decision-making as well, but are not physically connected to NARBHA's WAN. TAAs maintain a high degree of autonomy by choice, and NARBHA honors that decision. An invitation is always extended to TAA technical staff to attend the monthly collaborative meeting at NARBHA headquarters and they attend periodically, depending on the agenda items.

FFS and SCA providers submit only claims data to NARBHA, and thus do not need to be physically connected to the NARBHA WAN. Several FFS providers do, however, connect to NARBHA's File Transfer Protocol (FTP) servers to submit claims data via NARBHA's secure Virtual Private Network (VPN) concentrator.

NARBHA provides information systems-related technical assistance to the provider network MIS staff as resources permit. The NARBHA WAN Manager orients new SAA and TAA network administrators and information technology managers on their network connections to NARBHA and the greater WAN. All SAA locations participate in NARBHA's e-mail system; their MIS staff are trained in use of the client components and how to troubleshoot messaging-related problems. NARBHA also assists SAAs with other complex troubleshooting issues when they arise. Regarding security, NARBHA conducts training for SAA technical staff and provides ongoing support to resolve security issues. In addition, the NARBHA MIS Director and NARBHA WAN Manager assist the SAA information technology managers and directors in developing their own information systems policies and guidelines that make sense for their environments. Also, when FFS providers wish to submit claims data electronically, NARBHA MIS works with them to ensure that the process will work properly and sets up a VPN connection for their claims submission.

Electronic Clinical Systems Compatibility

NARBHA and its SAAs/TAAs use the same clinical system platform, the integrated clinical management system from CMHC Systems of Dublin, Ohio. This system, CMHC/MIS, is a comprehensive and flexible software solution for the behavioral health industry. NARBHA and its SAAs/TAAs use CMHC/MIS to manage administrative, financial, and clinical processing functions. As a result, users work more effectively and efficiently, facilitating quality care for NARBHA members**.**

The CMHC/MIS system has proven to be extremely flexible, providing additional components to meet NARBHA's business needs as a Managed Care Organization (MCO). It has worked equally well for the smaller, single catchment areas of NARBHA's SAAs/TAAs.

Of the nine SAAs/TAAs that NARBHA contracts with:

- Five SAAs use the fully integrated hardware/software implementations of the CMHC/MIS system at their respective sites.
- Two SAAs use the CMHC/MIS software hosted on NARBHA's hardware. Each SAA has its own separate, private data location on NARBHA's hardware.
- The two TAAs submit manual documents that are entered on their behalf by NARBHA staff into site-specific CMHC/MIS systems hosted on NARBHA's hardware.

NARBHA has designed an in-house program, Collection and Scanner Program/Edit Reporting (CASPER), for the Health Insurance Portability and Accountability Act (HIPAA)/834 enrollment and demographic data capture process. This application, made available to the SAAs free of charge, evaluates enrollment/demographic data submitted for completeness and consistency, eliminating errors at NARBHA and allowing the SAAs to resolve errors at their sites.

Each of the SAA/TAA systems listed above validates its enrollment, eligibility, and assessment data using the provider version of CASPER. After these data files are transferred via FTP from the site-specific CMHC/MIS systems back to NARBHA's central CMHC/MIS system, they are re-validated using NARBHA's MCO version of CASPER. This multiple validation process ensures a reliable import into NARBHA's CMHC/MIS system for single-source reporting and data repository.

Smaller SAAs and TAAs that do not have their own CMHC/MIS hosts, but instead use CMHC/MIS software on the host at NARBHA headquarters, follow the same procedures for collecting information, data entry, submission, and data validation as do the larger SAAs.

Handling of Electronic and Paper Submission

Realizing that a seamless and efficient exchange of information between NARBHA and the SAAs/TAAs is crucial, NARBHA has had robust processes in place to accept electronic data submission since FY 1997-1998. These original data submission processes comprised the ADHS/DBHS Client Information System (CIS) Intake, Closure, Assessment, Health Care Finance Administration Claim, Universal Billing 92 Claim, and Client Enrollment and Disenrollment Reporting (CEDAR) data.

These data submission standards were redesigned based on the October 2003 standard electronic transaction requirements of HIPAA and the ADHS/DBHS modifications to the demographic data capture process in August 2003. These new systems have continued to support the seamless exchange of information between NARBHA and its providers. While NARBHA provides electronic means for data exchange, it also continues to provide the ability for manually submitted data to enter the data system(s).

<u>Benefit Enrollment and Maintenance/Enrollment and Closure (HIPAA 834) and ADHS/DBHS Demographic</u>

Based on NARBHA's contracting model, all members are enrolled through one of the nine SAAs/TAAs. Currently, 96% to 98% of these data come from the SAAs and are submitted electronically and validated through CASPER.

The remainder of the data come from the two TAAs. These are submitted to NARBHA via fax for manual data entry, which is accomplished within one business day of receipt. NARBHA is working with the TAAs to allow them to assume this data entry responsibility at their sites, through a VPN connection to NARBHA's FTP server, so as to better recognize any errors and correct them immediately.

No FFS or SCA provider formats or submits enrollment or demographic data to NARBHA because NARBHA's contracting model has delegated these functions to the SAAs/TAAs.

<u>Health Care Claims/Institutional and Professional (HIPAA 837I/P)</u>

All SAAs submit claim transactions to NARBHA electronically. In FY 2003-2004, electronic submissions comprised 91.1% of NARBHA's claim volume, up from 88.0% the previous fiscal year. Currently, electronic submission accounts for 98% of claims.

NARBHA's FFS and SCA providers submit a mix of electronic and paper claims, while TAAs submit only paper claims.

Paper claims are currently submitted manually in hard copy via U.S. mail or in-person delivery, with occasional exceptions allowing faxed claims submissions. Paper claims are entered by Finance Department staff into separate data-entry databases. The data are then converted to standard HIPAA health care claims/institutional and/or professional for processing. In the event that problems with a manually submitted claim preclude its data entry, the errors are noted on transmittal documents and returned to the provider for correction and resubmission.

NARBHA has a process to assist FFS providers that wish to begin submitting electronic HIPAA Health Care Claims/Institutional and Professional (HIPAA 837/I and HIPAA 837/P). As each FFS provider is able to prove its ability to generate, consistently and correctly, the electronic HIPAA claims transactions, it is allowed to migrate from the manual process to electronic submission. NARBHA also will continue to support the manual submission process and will continue to assist, through data specification definition, testing, and secure data submission processes, any provider who wishes to migrate to an electronic claim submission footing.

NARBHA Pharmacy Billing

Retail pharmacy claims are submitted to NARBHA electronically by its Pharmacy Benefits Management firm, CaremarkPCS. This data submission process has been in place for the last decade and covers 100% of pharmacy claims. There are instances when CaremarkPCS accepts hard copy documents for pharmacy claims. It is the responsibility of CaremarkPCS to enter this information into its systems and pass those data to NARBHA electronically.

As noted in Volume 5.k of this RFP, NARBHA is working with CaremarkPCS to capture and submit retail claims supplemental information. NARBHA's intention is to tie the supplemental data capture process to the existing pharmacy claims process, thus capturing all supplemental data electronically along with the retail pharmacy claims.

Compatibility with Provider Systems

In addition to ensuring a seamless flow of data between NARBHA and its providers as detailed above, NARBHA provides system compatibility with its providers in the following areas.

Videoconferencing Compatibility

In 1996, NARBHA implemented Arizona's first telemedicine network, NARBHAnet, with a videoconferencing bridge and six endpoints with private, point-to-point T1 connections carrying the video signal between sites. Since then, NARBHAnet has grown to 17 endpoints (5 at NARBHA's Flagstaff headquarters and 12 at SAA clinical locations), has provided more than 18,000 clinical sessions, and has been recognized as a national leader in telemedicine.

Wide Area Network Compatibility

The Wide Area Network (WAN) was initially conceptualized with the full cooperation of NARBHA's SAAs in 1996 to share NARBHA's original videoconferencing network infrastructure. With its core site at NARBHA's Flagstaff headquarters, the WAN has now grown well beyond the videoconferencing infrastructure to 6 intermediate sites (directly connected to the NARBHA core site) and 18 edge sites (directly connected to intermediate sites) at SAA locations throughout Northern Arizona. (Refer to Diagram 5.d.2.) Private, point-to-point T1 circuits connect video, voice, and data traffic through static bandwidth allocation. This fiscal year, dynamic bandwidth allocation will be implemented at each location as NARBHA and its SAAs move to an integrated, IP-based model for video, voice, and data services. This will greatly enhance bandwidth performance to all remote sites. All of the SAAs recognize the benefits of this technological change and are entirely supportive of this transition, while being fully aware of the costs and complexities involved.

E-mail Compatibility

NARBHA MIS centrally administers a corporate e-mail system on behalf of NARBHA and all SAAs; this system includes separate e-mail post offices, message transfer agents, corporate Instant Messaging, Secure WebAccess, and Simple Message Transfer Protocol (SMTP) gateway services. NARBHA implemented the corporate e-mail infrastructure with the full cooperation of its SAAs in 1998. The corporate e-mail infrastructure includes all SAA endpoints on the WAN and consists of 1,189 user accounts, 808 external user accounts, 22 resource objects, 115 distribution lists, 2 document management libraries, 17 internal post offices, and 8 messaging domains. All components of the corporate e-mail system are located within NARBHA's private WAN, positioned safely behind NARBHA's SPAM filters, firewalls, and virus scanners. This means that all e-mails between NARBHA and the SAAs, or among SAAs, are secure.

TAAs and other providers that are not physically part of NARBHA's WAN (FFS and SCA providers) send e-mail via the Internet. Policies forbid NARBHA or any of its providers from sending Protected Health Information via Internet e-mail because it is not guaranteed secure; these policies are reinforced by training for all users.

Internet Access Compatibility

NARBHA provides centralized Internet access to NARBHA and the SAAs through two dedicated T1 direct Internet connections to its ISP, Qwest Communications. This allows for 3Mbps of concurrent Internet bandwidth. In addition to the 3Mbps, NARBHA employs a Cisco Content Engine that provides content caching of Internet traffic, increasing throughput by approximately 50%, creating a theoretical bandwidth speed of 4.5Mbps.

NARBHA has dedicated significant resources to providing a secure centralized Internet access point for NARBHA and its SAAs, and provides the following additional security services:

- Fully stateful (every packet is carefully screened) packet inspection of all incoming and outgoing Internet data ensures that business-related traffic is allowed, while traffic from unauthorized sources is discovered, logged, and dropped.
- Packet filtering of all incoming and outgoing Internet traffic ensures that unwanted data traffic is dropped and never makes it to NARBHA's WAN.
- Virus scanning of all incoming and outgoing Internet traffic ensures that NARBHA and its SAAs are protected, and are also good Internet neighbors, by not potentially spreading viruses to others.
- Content filtering of all incoming and outgoing Internet traffic looks at the actual content of packets to ensure that no illicit material is being relayed by NARBHA's network, and that no inappropriate web pages or e-mail are allowed inside.

Remote Access Compatibility

NARBHA provides remote access services to entities that are not physically part of the WAN through a Cisco 3005 Virtual Private Network (VPN) Concentrator. The VPN Concentrator allows properly configured and authorized users to access the NARBHA WAN over the Internet with 168-bit 3DES (triple DES) encryption technology that exceeds the industry standard. This provides an extremely secure method for NARBHA staff and/or contractors to work from remote site(s) or for FFS providers to retrieve data or submit claims to NARBHA. Through the concentrator, user accounts are tightly controlled as to what they can access on the WAN and when they can access it. This device supports both transport-layer and application-layer encryption. The concentrator also allows for undisrupted secure emergency communications to NARBHA's SAAs/TAAs or ADHS in the event of private line outages throughout the state. In addition to the VPN concentrator, NARBHA provides the ability for each of the SAAs to access its own hosts remotely and securely over the Internet through the use of an encrypted Microsoft Terminal Services connection.

Intranet and Extranet Compatibility

NARBHA's Intranet and Extranet allow it to instantly and securely disseminate easily accessible information to targeted groups through the NARBHA website at www.narbha.com. Intranet services cover the NARBHA WAN and are employed to disseminate information quickly and consistently within and among departments at NARBHA headquarters as well as to distribute information to the SAAs. Unique user accounts provide access control to specific locations on the website, so that information posted on the Intranet is accessed only by the target audience. Extranet services, or NARBHA web-based services accessed over the Internet by FFS providers, feature 128-bit Secure Sockets Layering (SSL) connectivity and also require authentication for access control within the website. To facilitate secure access using this technology, NARBHA MIS sets up user accounts for FFS providers when contracts are issued and instructs the providers to contact MIS to receive the training and passwords necessary to use this secure resource.

File Sharing Compatibility

NARBHA employs Microsoft Office XP Professional on each desktop, including Access, Excel, PowerPoint, and Word. This is fully compatible with all SAA locations. In the unlikely event of a conversion issue, select PCs used by key NARBHA administrative personnel are loaded with various software packages that allow NARBHA to translate files from standard business applications.

NARBHA provides two File Transfer Protocol (FTP) servers for exchanging data, software, and reports with its SAAs and those FFS and SCA providers that have been authorized to submit data to NARBHA electronically. SAAs access the FTP servers through their private, point-to-point T1 connections to NARBHA. FFS/SCA deposit claims data to the

FTP servers through NARBHA's Virtual Private Network (VPN) concentrator, which allows encrypted data transmission. Individual user accounts and file permissions ensure security among the various users.

NARBHA's Local Area Network (LAN) and Wide Area Network (WAN) are carefully planned and integrated for high performance, and are designed utilizing industry best practices. NARBHA has devoted considerable resources to ensure that a state-of-the-art, reliable, scalable, efficient, and secure infrastructure is in place to meet the needs of NARBHA and its Service Area Agencies and Tribal Area Agencies (SAAs/TAAs). Headquartered in Flagstaff, this network covers 62,000 square miles and five counties and serves approximately 1,300 employees in Northern Arizona. The network is designed to facilitate and promote NARBHA's primary mission of overseeing behavioral heath services in both rural and urban environments.

The following section details NARBHA's LAN, WAN, secure external connections, telemedicine network, and network security. LAN, WAN, and telemedicine network architecture diagrams are also included.

NARBHA Local Area Network Configuration

The LAN infrastructure serves NARBHA's 38,000-square-foot headquarters building and connects all NARBHA users to each other and to data network resources such as servers. For details on the LAN architecture, please refer to Diagram 5.d.1. This Gigabit Ethernet LAN consists of a single Main Distribution Facility (MDF) and four Intermediate Distribution Facilities (IDFs). Multiple redundant Gigabit fiber optic trunks connect the MDF to each IDF. The IDFs contain 22 Dell PowerConnect 5224 Gigabit Ethernet switches that interconnect 380 live Gigabit Ethernet ports throughout the facility. This allows NARBHA users to transfer data to and from other PCs at full Gigabit speed. All cabling is professionally tested and certified within the EIA/TIA-568-A standard for reliable Gigabit Ethernet speeds.

A Foundry FastIron 800 Core Gigabit Ethernet Switch provides a single backplane that connects users directly to network resources on the servers. This innovative design bypasses the traditional tiered-switching employed for server connectivity to the greater data network, thus avoiding the data bandwidth bottleneck that is encountered in many data network environments. Another design feature of the FastIron Switch further enhances data transmission speed. Each blade in the FastIron Switch is controlled by its own Application-Specific Integrated Circuit, which allows servers connected to the same blade to interface with each other without adding to data traffic on the backplane.

NARBHA Wide Area Network Configuration

NARBHA's WAN covers NARBHA headquarters (the core site) and 24 SAA locations throughout Northern Arizona. The 24 SAA locations consist of 6 intermediate sites (locations with direct connectivity to NARBHA headquarters) and 18 edge sites (connecting directly to the intermediate sites and, through them, to NARBHA's core site). Private, point-to-point T1 circuits connect video, voice, and data traffic throughout the WAN. The WAN infrastructure, consisting of telecommunications and routing hardware, enables secure and efficient communications among NARBHA and its SAAs.

In FY 2004-2005, NARBHA will implement dynamic bandwidth allocation at each location as it moves to an IP-based model for video, voice, and data services. This will greatly enhance bandwidth performance and efficiency to all remote sites.

The core site is physically located in Flagstaff. NARBHA's secure enterprise data center has its own air-conditioning facilities with false floor, independent electrical facilities, and an Inergen fire suppression system. All components of the data center adhere to the ANSI/TIA/EIA-569-A Standard for Telecommunications Pathways and Spaces. The data center is populated with telecommunications, video, voice, and data facilities.

- Telecommunications hardware Telecommunications hardware consists of a fully redundant DS3 cabinet. The DS3 is a fiber optic line that carries the equivalent of 28 T1 lines. DS3, as opposed to multiple T1s, provides the efficiency of expedited scalability and a significant overall cost savings. The DS3 coming into NARBHA's Flagstaff headquarters is channelized (divided) into 28 T1 (1.544Mbps) circuits by an Adtran MX2800 M13 multiplexer unit with fully redundant processor card. These T1 circuits carry video, data, and voice signals. Approximately 30 analog phone lines provide emergency voice, fax, and modem access in the unlikely event of a DS3 failure. Currently, a NET Promina 800 Integrated Services Digital Network (ISDN) Switch and Frame Relay Access Device provides Frame Relay and ISDN switching services, sending data and video signals to the NARBHA core router and videoconferencing bridge. The Promina and videoconferencing bridge are scheduled for replacement in FY 2004-2005 concurrent with a planned video protocol switch from ISDN to Internet Protocol (H.323, or video over IP). All telecommunications and WAN-related equipment is supported by battery backup and features redundant power supplies. As the network moves forward, all new telecommunications hardware will be purchased in accordance with a five-year life cycle.

- Data traffic is transmitted to a high-end Cisco 7206vxr core router. This device is responsible for providing data routing among NARBHA headquarters, NARBHA's SAA locations, the Internet, and ADHS/DBHS. Access control lists (ACLs) implemented on this core router and all other routers in the NARBHA data network provide packet-level security. By employing ACLs, each data packet header is scanned for a specific type of traffic, and is either permitted or denied through the router. Additionally, by utilizing fully private, point-to-point, dedicated T1 lines, NARBHA is able to reduce exposure to breaches in confidentiality and ensure the integrity of the data traffic. This router is scheduled for an upgrade to a more powerful Cisco 7206 in support of IP-based video services in FY 2004-2005.

- Video traffic is transmitted to a V-Tel SmartLink Model 2020 videoconferencing bridge, which is capable of connecting up to 20 video endpoints simultaneously. The bridge also can "cascade" with other bridges statewide to run extremely large, multi-site videoconferences. NARBHA will replace this videoconferencing bridge in FY 2004-2005 with an IP-capable Polycom Accord MGC-100 bridge, which will allow dynamic bandwidth allocation and video call compression throughout the NARBHA network, making more efficient use of existing network bandwidth and averting the need to install additional T1 lines. The new bridge also will allow further video network expansion and connection of more video sites simultaneously.

- Voice traffic is transmitted from the MX2800 multiplexer through a single T1 to two Mitel 200 Hybrid PBX telephony switches. These switches are interconnected with a trunk card and provide voice services for the NARBHA headquarters. A Meridian managed voice-mail server interfaces with the Mitel 200 switches as well, providing a flexible, modular, and scalable voice communications system that includes such features as centralized voice mail, paging, caller ID, multiple lines per user, and centralized attendant.

The intermediate sites are SAA locations with direct connectivity to NARBHA headquarters. Intermediate sites currently employ Cisco 2501 routers, although upgrades to Cisco 3600 routers are scheduled for in FY 2004-2005 in support of IP-based video services.

The edge sites provide connectivity to SAA remote networks from their respective intermediate sites. Currently, these edge sites also employ Cisco 2501 routers, but upgrades to Cisco 2651 routers are scheduled in FY 2004-2005 in support of IP-based video services.

Data Services Provided to External Entities

NARBHA's Management Information Systems Department (MIS) provides several data services beyond the WAN to ensure efficient communications among NARBHA, its SAAs, ADHS, and other entities. Services provided by NARBHA include: Internet access, Enterprise Messaging, File Transfer, Intranet and Extranet services, as detailed in Section 5.c.

- NARBHA provides secure, centralized Internet access to its SAAs through two T1 direct Internet access connections. This allows for 3Mbps of concurrent Internet bandwidth. Full stateful firewalling and virus scanning are performed on all Internet traffic.

- NARBHA provides centralized administration of Enterprise Messaging services for its SAAs, including e-mail post offices, message transfer agents, corporate Instant Messaging, Secure WebAccess, and Simple Mail Transfer Protocol (SMTP) gateway services.

- NARBHA provides two File Transfer Protocol (FTP) servers for transmitting data, software, and reports to and from its SAAs. Individual user accounts and file permissions ensure security among the SAAs.

- NARBHA provides Intranet and Extranet services through its website, www.narbha.com. NARBHA MIS employs Content Distributor, a content management system, to control access to specific locations on its website through user accounts, allowing NARBHA to immediately disseminate information to selected internal and external users. NARBHA's Intranet services allow exchange of interdepartmental information within NARBHA headquarters as well as consistent distribution of information to the SAAs. Secure Extranet services, allowing outside stakeholders easy access to necessary information on the NARBHA website, feature 128-bit Secure Socket Layer (SSL) connectivity and also require authentication for access control within the website.

- NARBHA provides remote access services to fee-for-service (FFS) agencies, SAA/TAAs, and remote users through a Cisco 3005 Virtual Private Network (VPN) Concentrator. Additionally, NARBHA provides a terminal services passthrough, which allows SAA MIS staff to remotely access and manage their key servers securely from anywhere in the Internet.

NARBHA Telemedicine Network Configuration

NARBHA's telemedicine network shares the WAN infrastructure, with NARBHA's Flagstaff headquarters housing the hub videoconferencing equipment, connected to the SAA videoconferencing endpoints via the same dedicated, private, point-to-point T1 telecommunications lines that also carry data signals.

Hub Equipment: NARBHA owns a V-Tel Model 2020 videoconferencing bridge, which is capable of connecting up to 20 video endpoints simultaneously and also can "cascade" with connected videoconferencing networks to accommodate large, statewide meetings. NARBHA also owns a NET Promina 800 ISDN and Frame Relay Switch, which sends video and data signals to the correct locations on the network. NARBHA is scheduled to replace both the V-Tel bridge and Promina 800 in FY 2004-2005 as part of a network-wide shift to the newer H.323 video protocol, or video over IP. NARBHA's new bridge will be an Accord MGC-100, which has significantly more power and functionality than the current bridge. The new bridge, along with enhancements to NARBHA's core 7200-series Cisco router, will take over the current functions of the Promina.

Endpoint Equipment: NARBHA's Flagstaff headquarters contains five videoconferencing rooms, two with Polycom Quad BRI codecs, and three with Polycom Viewstation FX codecs, all of which are capable of running video over IP (H.323 protocol). The NARBHA hub is connected to six SAAs in five counties with 12 video sites, most of which are IP-capable Polycom Viewstation FXs. Four endpoints employ older CLI video equipment and will upgrade to IP-capable systems concurrently with the network move to H.323 video protocol. Each video endpoint is allocated at least seven video channels on the 24-channel T1 lines; most are allocated nine channels to allow 512K conferences. The network standard is 384K for videoconferences. Remaining channels on the T1 lines are allocated for data. The network shift to H.323 will allow dynamic allocation of bandwidth; that is, bandwidth is allocated to function based on a prioritized list which is video first, voice second, and data third.

External Video Network Connections: In addition to direct connections between NARBHA and its SAA endpoints, NARBHA's videoconferencing hub is connected via full T1 lines to the following networks for videoconferencing only (no data transmissions).

- The ADHS/DBHS building in Phoenix, which allows video connections from NARBHA to:
  - DBHS (1 video endpoint)
  - The Community Partnership of Southern Arizona (CPSA) telemedicine network (25 video endpoints, 2 bridges, network hub in Tucson)
  - The Arizona State Hospital (5 video endpoints in Phoenix)
- The Arizona Council and Foundation for Human Service Providers (1 video endpoint in Phoenix)
- Pinal Gila Behavioral Health Authority (9 video endpoints, 1 bridge, network hub in Apache Junction)
- The EXCEL group (8 video endpoints, network hub in Yuma)
- The University of Arizona's Arizona Telemedicine Network (80+ video endpoints, 2 bridges, network hub in Tucson)
- Qwest Communications, for videoconferences involving off-network sites anywhere in the world

Network Utilization and Background

NARBHA's telemedicine network is used for doctor-patient visits; administrative meetings among NARBHA, its SAAs, the other RBHAs, and ADHS/DBHS; and training/educational meetings including Continuing Medical Education Units delivered through NARBHA's connection to the University of Arizona. Clinical sessions are assigned the highest priority on the network.

Information Systems Security

NARBHA practices “defense in depth” (that is, layer upon layer of network security measures) within all of its information systems, utilizing a standards-based design philosophy. Protective security measures are implemented from the end-user desktop to the edges of the NARBHA WAN, ensuring the availability, integrity, and confidentiality of all electronic information that is stored or transmitted.

Virus Scanning: Each workstation and server in the NARBHA network runs current antivirus software that is updated nightly. Server software scans all files that are accessed or copied to mass disk storage. Any device found infected with a virus is quarantined, cleaned, and then reintroduced to the protected network. A virus scanning and content-filtering appliance scans and cleans all inbound and outbound Internet traffic, including e-mail, hypertext, and file transfers. By policy, Internet Instant Messaging products are prohibited and blocked.

Spam Filtering: A spam filtering appliance blocks inbound traffic that appears on a regularly updated database of known spam sites or a “blacklisted” domain name. In the event of “false-positives,” domains or sites may be manually added to a permit list.

Remote Access and Encryption: NARBHA maintains a Cisco 3005 VPN Concentrator, allowing secure remote connectivity of up to 250 users. Each remote PC connects through the Cisco Universal Client, which features an “always on” stateful personal firewall, allowing for connections only when using 168-bit 3DES encryption. A stateful firewall inspects each and every data packet (instead of only the first packet in a series) for potentially compromising content. Protected Health Information is not authorized on remote PCs, nor may this information be transmitted unencrypted over the Internet. NARBHA users may access their mailboxes remotely through a 128-bit SSL Secure WebAccess interface.

User Education: New employees are oriented in safe computing practices that are outlined in NARBHA’s policies and procedures. Major topics include: responsible and secure e-mail use, secure password practices, desktop security and screen locks, file storage procedures, introduction of removable media to the protected network, and virus prevention and detection. Existing employees are periodically updated and reminded of safe computing practices at all-staff meetings. Additionally, mandatory training on Heath Insurance Portability and Accountability Act (HIPAA) regulations regarding privacy and security is routinely performed.

Firewalling: NARBHA employs a Cisco 506e primary firewall and access control lists on all routers to achieve filtering from the logical layer to the application layer. Stateful packet filtering is employed at the firewall and every router in NARBHA’s WAN is configured to filter select traffic types.

Intrusion Detection/Prevention: Currently, NARBHA uses GFI LANguard Network Security Scanner to ensure that recent security patches have been deployed on PCs and servers as well as checking network hosts for common vulnerabilities. In FY 2004-2005, Cisco’s SecureIDS stateful network intrusion detection system will be deployed as software code running on the new core router.

Logging and Auditing: NARBHA recognizes the value of collecting system audit information, as well as maintaining and reviewing system audit reports. Through careful weekly review of audit logs, NARBHA’s data networking professionals are able to protect sensitive information by identifying threats from both inside and outside the organization. There is no single solution that can interface with all information systems components to provide audit trails and logging, so NARBHA has employed several best-in-class auditing products. These are:

- SCO UNIX-SCOadmin Audit Manager: Provides host-level auditing for Server CMHCHOST.
- CMHC DBAudit: Performs detailed auditing of NARBHA’s mission-critical database application.
- Microsoft Windows Server and Novell NetWare-BlueLance LT Auditor+ V8.0 SP3: Performs auditing functions for all NetWare and Windows servers in NARBHA’s data network environment.
- Kiwi SysLog Daemon 6.1.0: Captures audit trails from key data network hardware such as routers and switches, which are configured to log, display, and forward information to a system logging (SysLog) server for centralized log inspection.

Disaster Recovery: Each night, tape backup software captures all files that have changed. Each week, all servers are backed up in their entirety and the backup media is taken to off-site storage to safeguard against a catastrophic event that may damage or destroy mission-critical data. Each backup program includes the capability of a “bare-metal restore,” affording timely recovery of critical business operations in the event that hardware has been destroyed and subsequently replaced. All switch and router configurations and operating systems are routinely saved to a file server after each change. NARBHA employs standard PC hardware and software builds, allowing replacement PCs to be quickly and consistently loaded with the image of the standard software build. A VPN concentrator allows for undisrupted secure emergency communications to NARBHA's providers or ADHS in the event of private line outages throughout the state.

Network Configuration and Architectural Drawings

Diagrams 5.d.1 through 5.d.4, below, depict NARBHA's LAN, WAN, and telemedicine network configurations.

Diagram 5.d.1: NARBHA LAN Configuration

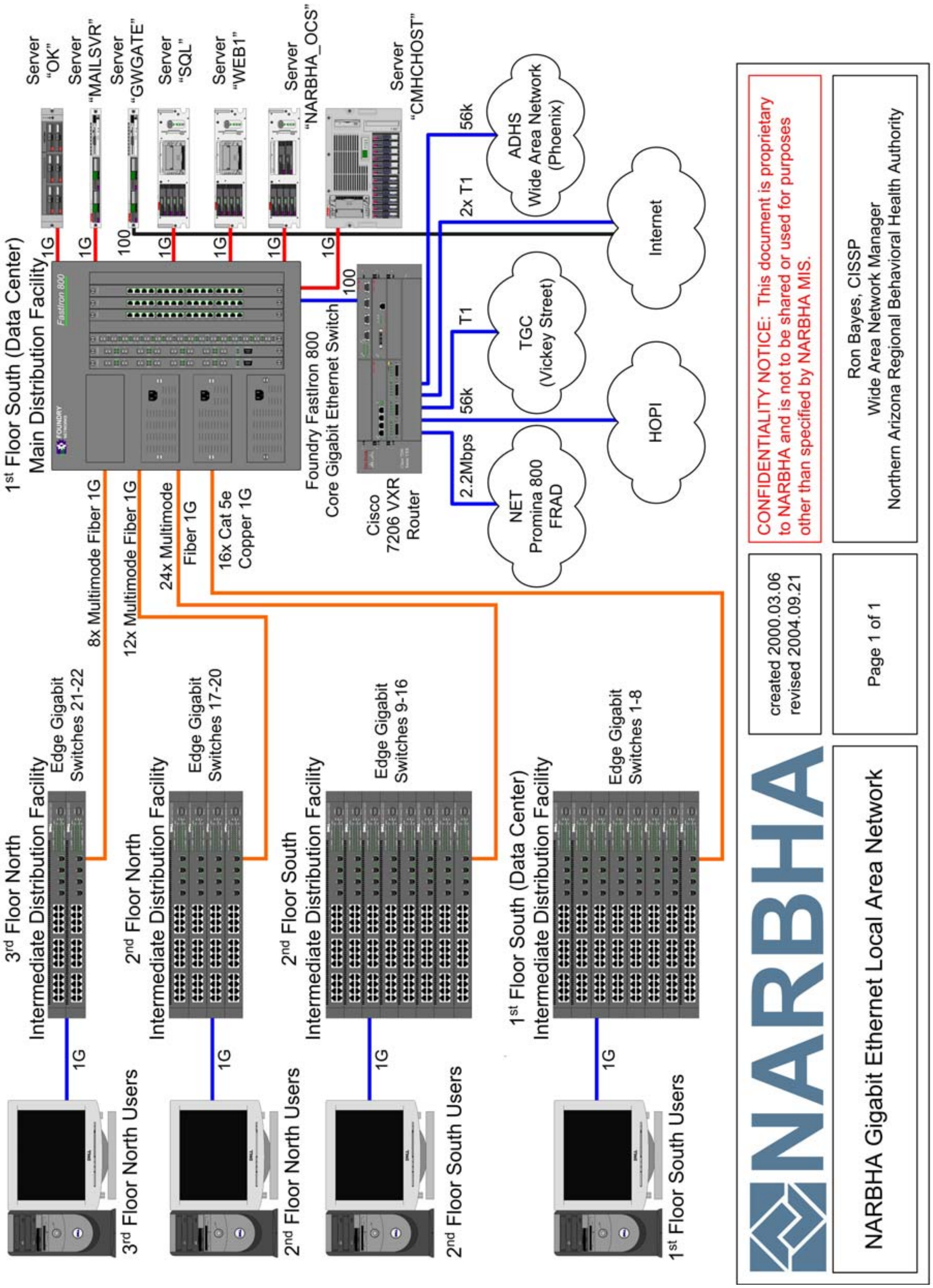
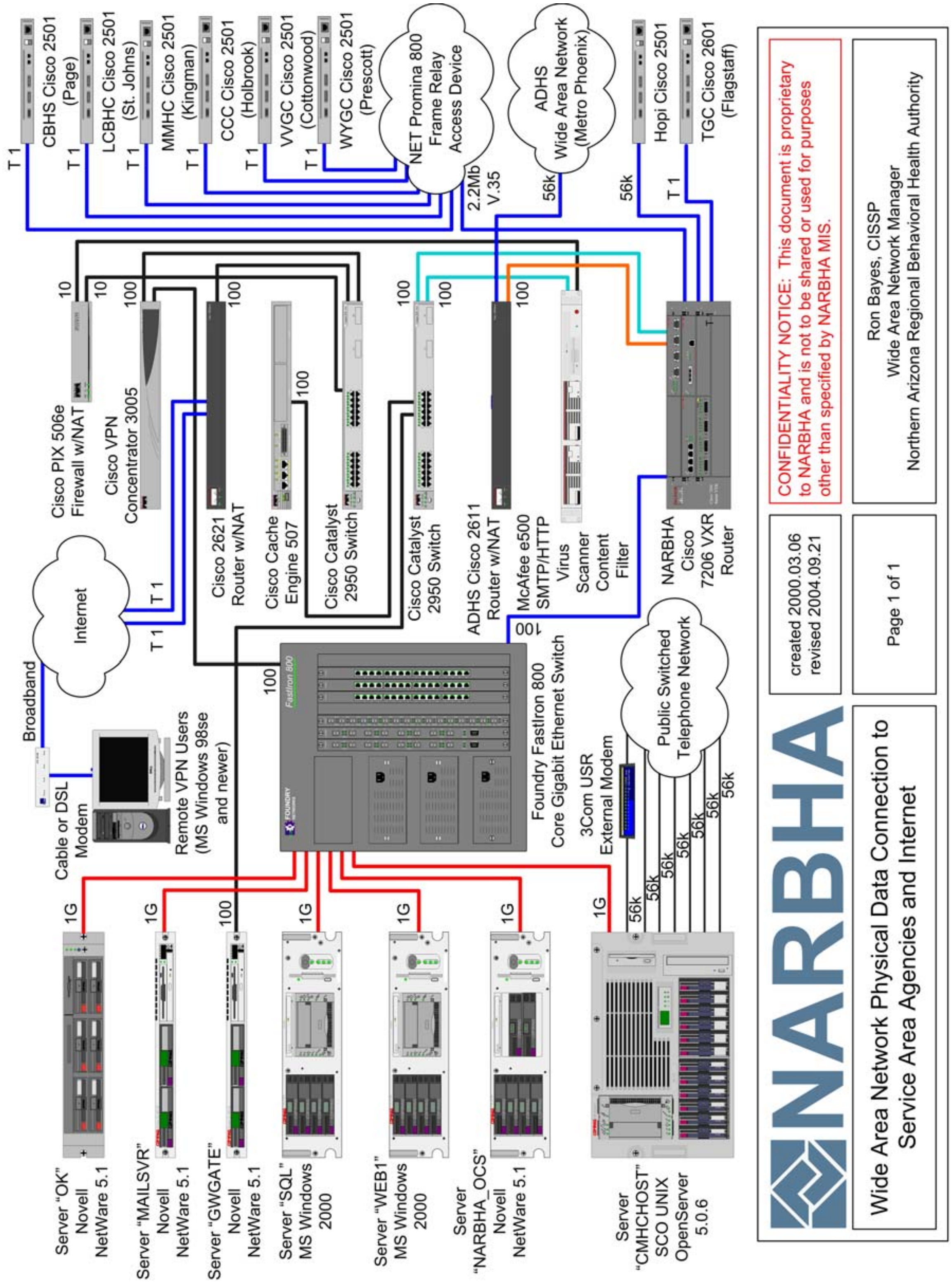
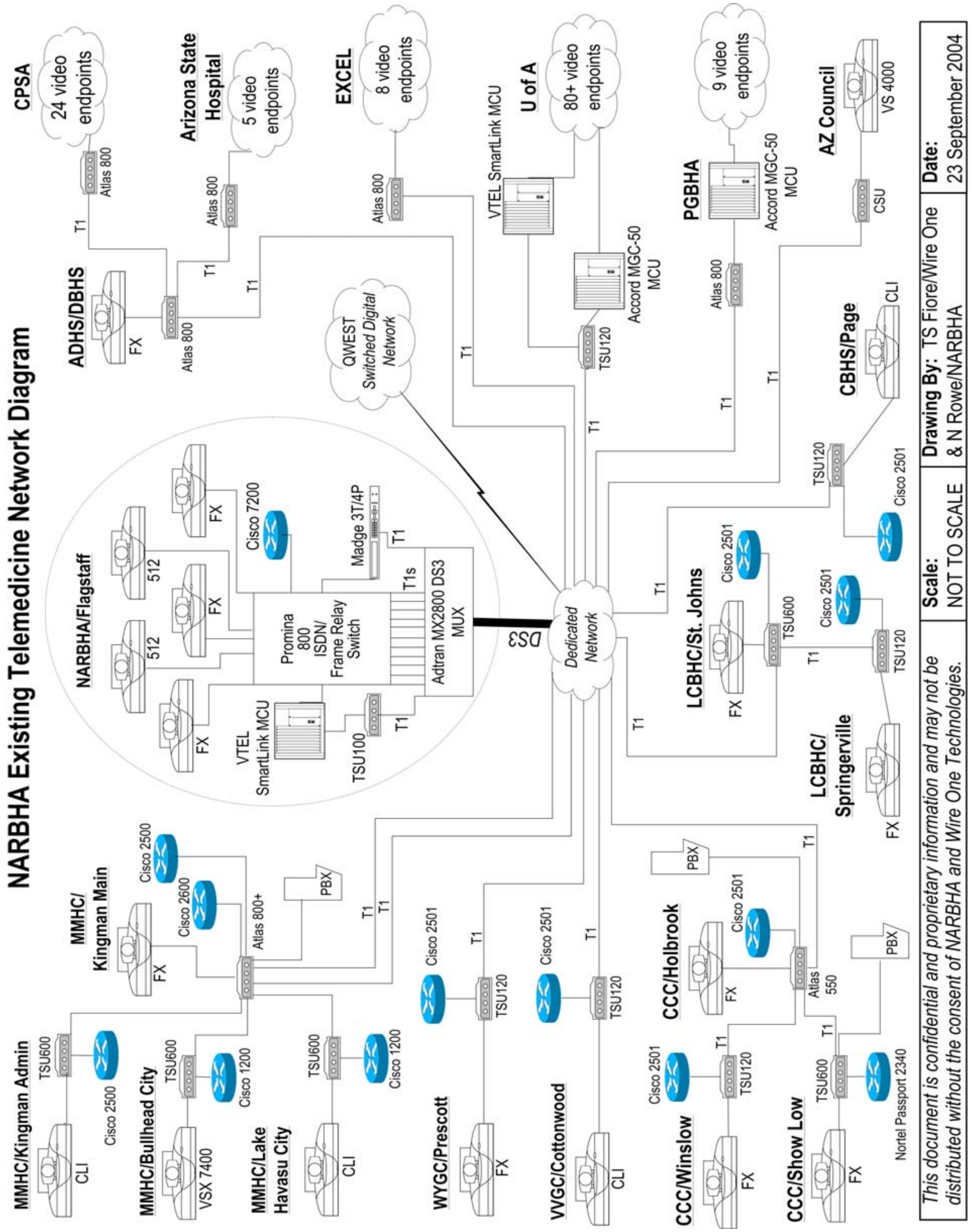

Server "OK"
Server "MAILSVR"
Server "GWGATE"
Server "SQL"
Server "WEB1"
Server "NARBHA_OCS"
Server "CMHCHOST"
1G
1G
100
1G
1G
1G
1G
100
1st Floor South (Data Center) Main Distribution Facility
FastIron 800
Foundry FastIron 800 Core Gigabit Ethernet Switch
Cisco 7206 VXR Router
56k
2x T1
T1
56k
2.2Mbps
ADHS Wide Area Network (Phoenix)
Internet
TGC (Vickey Street)
HOPI
NET Promina 800 FRAD
8x Multimode Fiber 1G
12x Multimode Fiber 1G
24x Multimode Fiber 1G
16x Cat 5e Copper 1G
3rd Floor North Intermediate Distribution Facility
Edge Gigabit Switches 21-22
2nd Floor North Intermediate Distribution Facility
Edge Gigabit Switches 17-20
2nd Floor South Intermediate Distribution Facility
Edge Gigabit Switches 9-16
1st Floor South (Data Center) Intermediate Distribution Facility
Edge Gigabit Switches 1-8
1G
1G
1G
1G
3rd Floor North Users
2nd Floor North Users
2nd Floor South Users
1st Floor South Users
CONFIDENTIALITY NOTICE: This document is proprietary to NARBHA and is not to be shared or used for purposes other than specified by NARBHA MIS.
created 2000.03.06
revised 2004.09.21
NARBHA
Ron Bayes, CISSP
Wide Area Network Manager
Northern Arizona Regional Behavioral Health Authority
Page 1 of 1
NARBHA Gigabit Ethernet Local Area Network

Diagram 5.d.2: NARBHA WAN Configuration


CBHS Cisco 2501 (Page)
LCBHC Cisco 2501 (St. Johns)
MMHC Cisco 2501 (Kingman)
CCC Cisco 2501 (Holbrook)
VVGC Cisco 2501 (Cottonwood)
WYGC Cisco 2501 (Prescott)
T 1
T 1
T 1
T 1
T 1
T 1
NET Promina 800 Frame Relay Access Device
2.2Mb V.35
ADHS Wide Area Network (Metro Phoenix)
56k
Hopi Cisco 2501
56k
TGC Cisco 2601 (Flagstaff)
T 1
10
10
100
100
100
100
100
100
Cisco PIX 506e Firewall w/NAT
Cisco VPN Concentrator 3005
Cisco 2621 Router w/NAT
Cisco Cache Engine 507
Cisco Catalyst 2950 Switch
Cisco Catalyst 2950 Switch
ADHS Cisco 2611 Router w/NAT
McAfee e500 SMTP/HTTP Virus Scanner Content Filter
NARBHA Cisco 7206 VXR Router
Internet
T 1
T 1
Broadband
Cable or DSL Modem
Remote VPN Users (MS Windows 98se and newer)
100
100
Foundry FastIron 800 Core Gigabit Ethernet Switch
FastIron 800
FOUNDRY NETWORKS
3Com USR External Modem
Public Switched Telephone Network
56k
56k
56k
56k
56k
56k
56k
1G
1G
100
1G
1G
1G
1G
Server "OK" Novell NetWare 5.1
Server "MAILSVR" Novell NetWare 5.1
Server "GWGATE" Novell NetWare 5.1
Server "SQL" MS Windows 2000
Server "WEB1" MS Windows 2000
Server "NARBHA_OCS" Novell NetWare 5.1
Server "CMHCHOST" SCO UNIX OpenServer 5.0.6
CONFIDENTIALITY NOTICE: This document is proprietary to NARBHA and is not to be shared or used for purposes other than specified by NARBHA MIS.
created 2000.03.06
revised 2004.09.21
Ron Bayes, CISSP
Wide Area Network Manager
Northern Arizona Regional Behavioral Health Authority
Page 1 of 1
NARBHA
Wide Area Network Physical Data Connection to Service Area Agencies and Internet

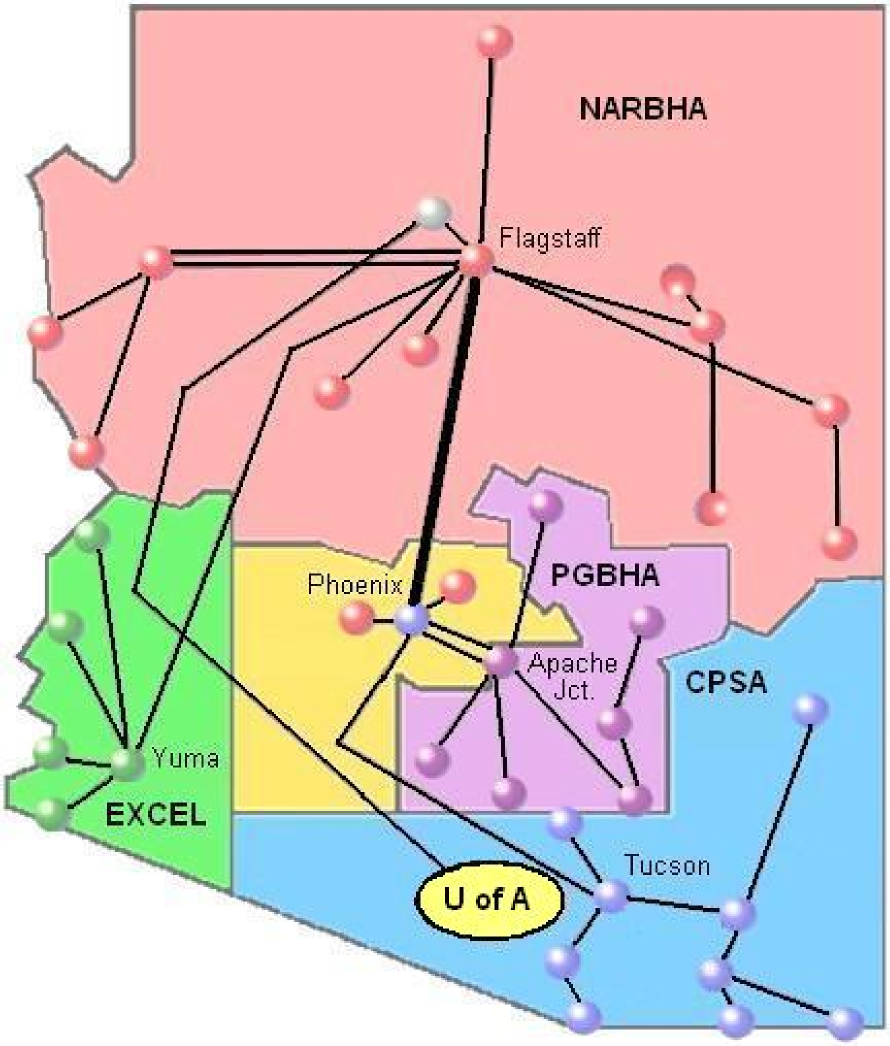
1 **Diagram 5.d.3: NARBHAnet Telemedicine Network Configuration**

2



3

Diagram 5.d.4: NARBHAnet and Connections to RBHA and University of Arizona Telemedicine Networks



NARBHA has had successful interfaces in place to allow transfer of electronic data between NARBHA systems and ADHS data systems since FY 1997-1998, and between NARBHA systems and DBHS data systems since FY 1998-1999. These implementations supported all aspects of data submission to and from the ADHS/Client Information System (CIS) and the DBHS/Client Enrollment, Disenrollment, and Assessment Reporting (CEDAR) systems. These electronic data interfaces were put into place in a security environment that adhered to ADHS/DBHS requirements at that time. NARBHA's long history of successful electronic data exchange with ADHS and DBHS provides a strong foundation for implementation of all required security features to comply with the Health Insurance Portability and Accountability Act (HIPAA) security standards by March 2005. As with all past changes to the data exchange process, NARBHA will work parallel to ADHS and DBHS to implement the necessary security features. During implementation of the HIPAA standard transactions in the fall of 2003, NARBHA was the first Regional Behavioral Health Authority (RBHA) to successfully test transactions with ADHS/DBHS.

HIPAA Security Standards Compliance

NARBHA's network and communications infrastructure includes many of the security features that are required by the HIPAA security standards. NARBHA will be in full compliance with all HIPAA security standards by March 2005, including the requirement that any Protected Health Information (PHI) must be encrypted when transmitted over the Internet or over an Extranet (business-to-business communication using Internet technologies) such that:

- The receiver is confident that the information came from the expected sender.
- The sender is confident that the data can only be used by the intended recipient.
- The data are unable to be changed in the transfer process.

Compliance with these HIPAA standards will also satisfy the requirements set in this RFP. HIPAA compliance in the area of data exchange will be accomplished through the implementation of software at NARBHA that allows for encryption of data using industry-standard encryption technology and the corresponding implementation of the technology necessary to support this encryption at ADHS/DBHS.

NARBHA has a dedicated, point-to-point 56K telecommunications line to ADHS that is used for electronic data transfer. During FY 2004-2005, NARBHA will replace this 56K circuit with a full T1 line.

Software Used for Electronic Data Transfers

NARBHA uses WS_FTP Professional, marketed by Ipswitch, Inc., of Lexington, Mass., to facilitate the transfer of data between NARBHA and ADHS/DBHS. NARHBA has implemented WS_FTP Professional as the standard method for electronic submission/transfer of data files between ADHS and NARBHA using File Transfer Protocol (FTP) in an unencrypted transfer, according to current ADHS/DBHS requirements. Upon successful testing of NARBHA's planned encryption technology at ADHS/DBHS, and agreement on an implementation date, NARBHA will implement the encryption technology at its site and begin using it as the standard method of data transfer.

Secure Electronic Data Interface

WS_FTP Professional is able to effect secure methods for data exchange using FTP with Secure Sockets Layer (SSL) technology. SSL technology uses 128-bit encryption, allowing for the creation of over 300 billion billion billion unique key combinations. SSL technology is implemented such that:

- A public key is issued by one party (ADHS/DBHS).
- A second party (NARBHA) uses that public key to encrypt the data and transfer them to the first party via FTP.
- The receiving party (ADHS/DBHS) uses a corresponding private key to unencrypt the information after receiving it.

The WS_FTP Professional program operates at NARBHA in two modes, each able to function at the encrypted (SSL) and unencrypted (non-SSL) level.

- For production/regular programs that transfer data to ADHS/DBHS on a regular basis, NARBHA has created a number of files, called scripts, which perform a series of pre-defined commands to effect the transfer of data between AHDS/DBHS and NARBHA systems. These scripts are created and tested the first time a specific file or series of files is exchanged with ADHS/DBHS, and used every subsequent time that same data are exchanged with ADHS/DBHS. Examples of these uses are the transfer of data for Institutional and Professional Claims, Enrollment Rosters, NCPDP pharmacy claims, and the ADHS Withhold files.

- For on-demand/ad hoc data transfer between AHDS/DBHS and NARBHA systems, NARBHA also uses WS_FTP Professional; however, in this mode it functions as a normal Windows program instead of an automatic script: the user identifies the system(s) to connect to, marks the data that need to be to exchanged, and executes the file transfer. Examples of these uses are transfers of the Inpatient Showing reports for the ADHS/DBHS Office of Quality Management and Financial E-Statements for the ADHS/DBHS Finance Department.

Refer to Volume 5.k. for complete data flow diagrams showing production data transfers between NARBHA and ADHS/DBHS.

FTP user IDs and passwords are issued to NARBHA by staff at ADHS/DBHS for these processes. It is the responsibility of the NARBHA MIS Director or designee to obtain, secure, and as necessary, change these User IDs and passwords. The transfer processes are built in such a manner that the user ID/password is issued to the process, or program, transferring the data, not to the staff member responsible for transferring the data. Logs of access are maintained by each unique process.

Using these programs and technologies, NARBHA is able to ensure that all data passed between NARBHA and ADHS/DBHS data systems are secure, that the information is unchanged, and that NARBHA or ADHS/DBHS can be confident of the source of the information.

NARBHA production systems are designed to support its business needs in a stable and reliable manner.

NARBHA tracks its system downtime data using the following definitions.

- Scheduled downtime means NARBHA's Management Information Systems Department (MIS) can plan for the system outage and implement alternate plans for access if necessary.
- Unscheduled downtime is due to hardware, software, or service failures.
- Non-critical systems are not necessary for NARBHA's core business to continue functioning. Examples of these are the E-mail system and Internet gateway.
- Critical systems are necessary to NARBHA's core business functions. These include the CMHC/MIS system, and file-sharing and printing services.

Total System Downtime

As the following tables show, NARBHA has experienced 116.8 hours of total downtime during the six-month period from March 1, 2004, through August 31, 2004. Total system downtime amounts to 2.6% of total hours in the six-month period, divided as follows.

- Critical system scheduled downtime—38.4 hours. The majority of this (23 hours) was a Claims Systems archive process that was scheduled well in advance of the actual date, allowing NARBHA to make plans for alternate data systems access.
- Critical system unscheduled downtime—5.4 hours
- Non-critical system scheduled downtime—0 hours
- Non-critical system unscheduled downtime—73.0 hours

Total Critical System Downtime

In the six-month period from March 1, 2004, through August 31, 2004, NARBHA experienced just 43.8 hours, or 0.99%, of critical system downtime. A critical system downtime factor of less than 1% is within industry standards.

- The majority of critical system downtime (38.4 hours) was scheduled, allowing NARBHA to plan for the outage and communicate the plan to end-users.
- Factoring out scheduled unavailability and looking only at non-scheduled events (emergencies), critical system downtime was only 5.4 hours, or 0.12% of total hours in the six-month period.

Production system servers

The downtime logs that follow refer to NARBHA production systems, which reside on seven servers connected through a robust, protected network infrastructure. Details of these servers are discussed in Volume 5.a. The production-related servers are:

- Novell Server "OK," providing *e*Directory root master replica, file services, plug-and-print services, desktop management services, backup services, and one messaging post office database
- Novell Server "NARBHA_OCS," providing *e*Directory root master replica, file services, UNIX print services, File Transfer Protocol (FTP) services, eight messaging post office databases, and instant messaging throughout the NARBHA/SAA data network
- UNIX Server "CMHCHOST," providing the platform for NARBHA's primary business services, the CMHC Management Information Systems (CMHC/MIS) application package, as well as File Transfer Protocol (FTP) services
- Windows 2000 Server "WEB1," providing secondary Domain Name Services (DNS), Active Directory domain controller, Dynamic Host Configuration Protocol (DHCP) services, subordinate Certificate Authority, secure web-based messaging interface (throughout the NARBHA/SAA data network), and system logging services (used for auditing security of network hardware
- Windows 2000 Server "SQL," providing primary DNS services, Active Directory domain controller, Root Certificate Authority, SQL database services, and secure web-based content distribution services
- Novell Server "MAILSRV," providing the primary message transfer agent for enterprise messaging
- Novell Server "GWGATE," providing enterprise messaging, Simple Message Transfer Protocol (SMTP) gateway services, and web-based enterprise messaging backend processing

System maintenance

In maintaining these systems and the network and telecommunication infrastructure, NARBHA MIS technical staff monitors system activity on a daily basis. When they note a problem, they either correct it immediately, if severe enough, or plan to resolve the issue at a later time or date.

Scheduled System Downtime

Scheduled system downtime is support or maintenance that can be planned for and performed in a fashion that eliminates or minimizes the impact on the user community. Examples are: application of patches to the clinical system (every Thursday from 7:00 a.m. to 8:00 a.m.); application of patches to the core or intermediate switches and routers that connect servers to the Local Area Network (LAN) and Wide Area Network (WAN) infrastructure and to staff personal computers, scheduled for non-business hours; archiving of historic claim data, performed as necessary and scheduled well in advance; and server replacement, scheduled for non-business hours.

Table 5.f.1: Scheduled System Downtime March 1 – August 31, 2004

Date	Reason for Downtime	Affected Services	Affected Server/Device	Total Downtime
3/4/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	45 Minutes
3/10/04	CMHC Patches loaded/ Database archive	CMHC/Behavioral System	Server CMHCHOST	8 Hours
3/18/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	10 Minutes
3/24/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	32 Minutes
4/1/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	18 Minutes
4/8/04	NO UPDATES			0
4/15/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	27 Minutes
4/22/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	27 Minutes
4/29/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	30 Minutes
5/6/04	NO UPDATES			0
5/13/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	18 Minutes
5/20/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	20 Minutes
5/27/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	20 Minutes
6/3/04	NO UPDATES			0
6/10/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	15 Minutes
6/16/04	CMHC Claim Archive	CMHC/Behavioral System	Server CMHCHOST	23.5 Hours
6/16/04	CMHC Patches loaded/ Database archive	CMHC/Behavioral System	Server CMHCHOST	11 Minutes
6/24/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	34 Minutes
7/1/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	10 Minutes
7/15/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	18 Minutes
7/22/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	25 Minutes
7/29/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	11 Minutes
8/5/04	NO UPDATES			0
8/12/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	21 Minutes
8/18/04	CMHC Patches loaded	CMHC/Behavioral System	Server CMHCHOST	23 Minutes
			Total Scheduled System Downtime	**38.4 Hours**

Unscheduled System Downtime

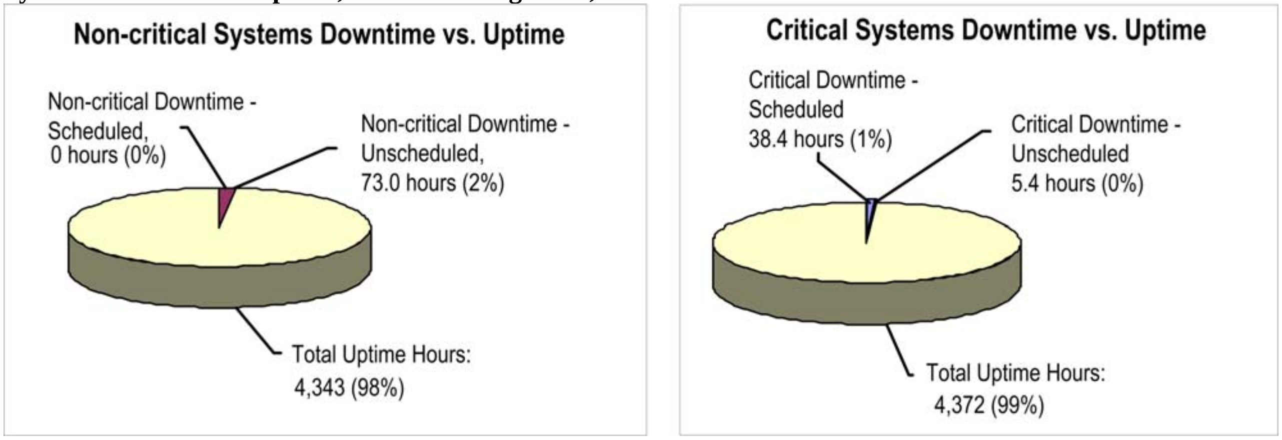
Unscheduled system downtime is support or maintenance that must be handled immediately because the system in question has “locked up” and is no longer available for staff use. Examples include print or E-mail services that stop responding to a user or administrator, where the only option is to restart the process. In these instances, the process is unavailable until restarted. Whenever possible, NARBHA users and the SAAs that co-exist on the NARBHA WAN are warned about unscheduled maintenance before it is done to provide them an opportunity to save documents or complete critical tasks.

Table 5.f.2: Unscheduled System Downtime March 1 – August 31, 2004

Date	Cause of Downtime	Affected Services	Affected Server/Device	Resolution	Total Downtime
3/1/04	Internal network traffic appears to be intermittent for some users	All services for multiple users	Dell Edge Switches	Buffer issue. Cold booted flash switch firmware.	1.5 Hours
3/2/04	E-mail not routing to internet	External E-mail	Server MAILSVR	Replaced RAID controller hardware.	27.5 Hours
3/5/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process	10 Minutes
3/8/04	Network printers down	Printing	Server OK	Restarted NDPS.	8 Minutes
3/11/04	Internal network traffic slow	All services	Foundry FastIron 800 Core Gigabit Switch	Trunking problem with fiber connections. Resolved with reconfiguration of the core switch.	2.6 Hours
3/16/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process.	10 Minutes
3/24/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process.	10 Minutes
3/24/04	Inbound Internet E-mail not received	Inbound Internet E-mail	Server GWGATE	Restart of message transfer alert. Cleared corrupt message.	10 Minutes
3/24/04	Inbound Internet E-mail not received	Inbound Internet E-mail	Server GWGATE	Restart of message transfer alert. Cleared corrupt message.	10 Minutes
3/24/04	Inbound Internet E-mail not received	Inbound Internet E-mail	Server GWGATE	Restart of message transfer alert. Cleared corrupt message.	10 Minutes
3/25/04	Inbound Internet E-mail not received	Inbound Internet E-mail	Server GWGATE	Software issue resolution through vendor. Patched faulty components.	13 Hours
5/6/04	Server Unresponsive, not allowing connections	1xE-mail Post Office, Some File Services, NDPS Print Services	Server OK	Possible virus scan issue. Volume repair, warm boot. Upgraded virus scan product.	3.5 Hours
5/19/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process.	10 Minutes
6/15/04	Server Unresponsive, not allowing connections	7xE-mail Post Offices, File Services, Printing Services on UNIX and NetWare	Server NARBHA_OCS	Warm boot. Cause not isolated.	10 Minutes
6/15/04	GWIA threads not releasing	External outgoing mail	Server GWGATE	Warm boot cleared GWIA process.	10 Minutes
6/24/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process.	10 Minutes
6/24/04	Static lock of host	CMHC	Server CMHCHOST	Cold boot restored CMHC program.	15 Minutes
7/19/04	Server Unresponsive, not allowing connections	7xE-mail Post Offices, File Services, Printing Services on UNIX and NetWare	Server NARBHA_OCS	Corrupt system volume. Volume repair, warm boot.	3.3 Hours

Date	Cause of Downtime	Affected Services	Affected Server/Device	Resolution	Total Downtime
7/19/04	No network connectivity for 3rd Floor North	All, but only for 3rd Floor North	Foundry FastIron 800 Core Gigabit Switch	Hardware failure of Management Module on core switch. Replaced hardware.	23.75 Hours
7/26/04	Process hung	1xE-mail Post Office, Some File Services, NDPS Print Services	Server OK	Warm boot released hung process.	10 Minutes
7/28/04	Server unresponsive	7xE-mail Post Offices, File Services, Printing Services on UNIX and NetWare	Server NARBHA_OCS	Cold boot. Cause not isolated.	20 Minutes
8/3/04	Locked process	CMHC	Server CMHCHOST	Warm boot cleared hung process.	10 Minutes
8/17/04	Server unresponsive	1xE-mail Post Office, Some File Services, NDPS Print Services	Server OK	Warm boot released hung process.	20 Minutes
8/23/04	Network printers down	Printing	Server OK	Restarted NDPS.	5 Minutes
				Total Unscheduled System Downtime	**78.4 Hours**

System Downtime vs. Uptime, March 1 – August 31, 2004



Parallel Systems

Testing server and infrastructure changes

Because the SAAs have their own stand-alone systems to capture and store data, separate test systems are not necessary for NARBHA's system servers, network infrastructure, and telecommunications infrastructure. Instead, NARBHA MIS applies patches and enhancements to the servers, network infrastructure, and telecommunications infrastructure as necessary after thoroughly reviewing the release documentation, determining the potential impact to the user community, and determining the benefit to the installation.

In the event that NARBHA MIS determines through research that an upgrade or patch could have an adverse affect on these systems, NARBHA MIS plans the implementation for off hours when no staff will be affected; ensures that full systems backups are available of the affected system(s); and applies the patches as defined in the documentation. Finally, MIS, through predefined scenarios, tests the patches to determine if they are functioning as defined by the vendor and functioning correctly in the NARBHA environment. If any patch is not performing as required, MIS staff remove the patch immediately and return the system to the previous software or hardware configuration, testing that configuration to ensure that it is working properly. The MIS staff then review the documentation, research the issue with the vendor, and reschedule the implementation for a future date.

If MIS has either determined that there is no possible negative impact of the patch on the systems or has implemented the patch as stated above and accepted it, MIS notifies the affected staff that changes have been implemented, defines how the changes may affect the end users, and asks that the end users, if they notice any negative impact, notify MIS immediately.

Testing programming changes

In the programming area, NARBHA has not defined additional test systems that reside on separate hardware, but instead has defined separate test systems on existing hardware that are used for testing of program and system changes. These systems consist of:

- A fully functional Managed Care Organization (MCO) data system within NARBHA's CMHC/MIS core business system, which is used to track member-level information. This test system can be configured to reflect the entire NARBHA production MCO system (for volume tests), or a portion of the MCO data system based on the scenarios to be tested.
- A fully functional Claims (CLM) data system within NARBHA's CMHC/MIS system. Again, this test system can be configured to reflect the entire NARBHA production CLM system,(for volume tests), or a portion of the CLM data system based on the scenarios to be tested.
- On the Novell network side, a full 60 gigabytes of mass storage to support the production program test environment, which is used to develop and test all Microsoft Visual FoxPro applications developed by MIS. The data sets for this test environment can be set to reflect the entire NARBHA non-CMHC file base (for volume tests), or just a portion of the non-CMHC file base based on the scenarios to be tested.

NARBHA MIS typically performs testing in parallel with current production systems, using real-time production data whenever possible. This allows the MIS department analyst to compare the results of the original production process to the modified test systems results to see if the modifications were successful. If the test results do not meet expectations, the MIS analyst has the test and production data sets available to research why the test failed, resolve the problem, and re-test the process. Upon review and acceptance of change by the MIS analyst, the changes are reviewed by the end users and again reviewed by the analyst. If the end user concurs that the modifications were successful and meet expectations, the program is transferred to the production environment for use. Operations staff who are running the new or modified process for the first time are assisted by MIS programming staff to see that the modification is working correctly.

For changes to complex systems, such as the Collection and Scanner Program/Edit Reporting (CASPER), a team of four to six MIS staff is set up under the direction of the lead analyst or manager responsible for the change. The team oversees any changes, definition of test scenarios, execution of test scenarios, data conversion (if necessary), and ultimate implementation at NARBHA and the SAAs. As part of this formal process, the team keeps design review minutes and task logs and holds regular meetings to review progress.

NARBHA's thorough testing of patches and enhancements prior to implementation, as well as NARBHA's thorough programming testing prior to implementation, ensures that both hardware and software systems are available and functional when needed.

NARBHA is committed to providing all of its employees with the appropriate skills needed to perform their duties. Training is an important component of maintaining an effective, efficient, and enthusiastic team. NARBHA's Management Information Systems Department (MIS) selects training that is appropriate to the needs of the organization and growth of the department, as well as to the professional enhancement of the individual employee.

NARBHA MIS meets its training goals by utilizing a three-tiered approach.

- First, the new employee is trained and oriented by their direct supervisor and through NARBHA's formal orientation process shortly after they are hired.
- Second, the employee receives continuing education through on-the-job training.
- Third, the employee receives formal training offsite, most often through an authorized education center.

New Employee Training/Orientation

New employee training thoroughly educates new MIS employees about NARBHA's business and corporate culture in several ways.

- Department-level training is performed first to get the new employee functional. This level of training includes NARBHA's data network environment, telephone system, security, HIPAA regulations/guidelines, and organizational structure.
- After initial departmental orientation, the employee is required to attend a two-day company orientation within the first month of employment. In this longer, more in-depth orientation, the employee is introduced to the general functions performed by each department at NARBHA, as well as many internal NARBHA policies and procedures. This creates a better understanding of the organization as a whole and its behavioral health care mission and processes. It also enables the new employee to help meet interdepartmental and company objectives.
- Specific day-to-day job responsibilities are learned through "shadowing" an experienced employee for up to two weeks. No employee is expected to "hit the ground running"; rather, the employee is gradually given more and more responsibility as he or she demonstrates proficiency in daily tasks.

On-the-Job Training

On-the-job training for MIS employees is handled by senior members of the team. One of the most important facets of job satisfaction and retention for information systems professionals is cultivation of a stimulating and challenging work environment. This is achieved primarily through on-the-job training by senior members of the team. Employees are slowly and methodically exposed to existing corporate technologies, as well as the "big picture" of NARBHA's behavioral health care management processes, through a mentoring process. Gradually, the employee is trained for the "next job," facilitating retention of a quality work force. Professional growth is always encouraged. Periodically, an employee is challenged with implementation of a new technology, or is requested to participate as a key figure within a high-exposure project. Each employee is provided the maximum opportunity to excel, and their subsequent achievements are recognized through the NARBHA Employee Recognition Program.

Cross training is another often-used technique for on-the-job training at NARBHA. MIS remains efficient through having multiple employees trained on any given task. While each employee has particular talents, abilities, and responsibilities, MIS achieves business continuity through other team members being able to perform those tasks at a functional level. For example, a programmer develops a new application for use by NARBHA or its provider network. The developing programmer trains a backup programmer on the design structure of the application during development and again at implementation. Users then direct functional (code-related) problems to the developing programmer or the backup programmer trained in the application. In some mission-critical applications, multiple MIS Staff are familiar with a particular job function.

Use of in-house resources allows MIS staff members to further their professional educations. Computer-based training is in use for the newest version of NARBHA's enterprise messaging system, allowing Help Desk professionals to become intimately familiar with the product and all of its capabilities. Each MIS employee maintains a fairly extensive library of text materials specific to his or her tasks. MIS staff are encouraged to order new reference materials; these resources are shared with other MIS staff as necessary. Additionally, programming staff have purchased and used training video libraries to understand and employ new features in the latest versions of a programming language.

Participation in NARBHA's provider improvement process
NARBHA's Provider Improvement Committee (PIC) is a multi-disciplinary team that acts on requests from NARBHA's Provider Performance Committee to develop and implement improvement plans for identified provider improvement opportunities. PIC is comprised of a minimum of two line staff members from each NARBHA department. The committee meets twice a month and presents a report on the progress of all ongoing improvement activities regularly to the Provider Performance Committee and to NARBHA's Leadership Council. At least two MIS staff members at a time are part of PIC; each staff member stays on PIC for at least a year. In this way, MIS staff are actively involved in, contribute to, and learn in detail about NARBHA's behavioral health care delivery processes and environment.

Participation in All-Staff Trainings
NARBHA's monthly all-staff meetings include trainings by various staff members regarding important facets of NARBHA's behavioral health care delivery system, such as the grievance and appeals process, Health Insurance Portability and Accountability Act (HIPAA) requirements, member rights, environment of care, corporate compliance, assessment standards, serious mental illness (SMI) eligibility, cultural competency, covered services, clinical operations, eligibility/enrollment screening/referral, fraud and abuse, interpreter services, and record review procedures.

Formal Offsite Training
NARBHA allocates significant resources to ensure that MIS staff has the most current training in support of NARBHA objectives. This often includes travel to a training site because NARBHA is headquartered in a rural community with limited training resources. Most offsite training takes place in Phoenix, although out of necessity MIS employees have visited other locations in the continental U.S. to receive high-end or accelerated training. Training goals and requirements for all NARBHA staff are identified in their annual performance appraisals; progress toward these goals is monitored by the Human Resources Department.

While training and certifications do not ensure competency, they are good indicators of staff exposure to different technologies. MIS staff have the opportunity to attend a minimum of one major vendor-authorized training event per year and may also receive additional training sessions as necessary. NARBHA typically pays for training and travel expenses, while the employee absorbs the costs of any certification or testing fees associated with the class. In an effort to ensure that NARBHA sees a return on investment with expensive training, the employee may be required to sign an agreement to remain employed at NARBHA for one full year following completion of the training or to reimburse NARBHA for the cost of the training. This requirement is applied at the discretion of the supervisor and/or the Director of Human Resources, and is based on the cost of the training and the skills the employee will gain from the training. After MIS employees have attended training, they are often challenged with additional responsibility relevant to their newly received training in order to employ their new skills. They also may be asked to impart what they have learned to their peers within NARBHA and its Service Area Agencies in a workshop-type setting.

Below is a list of vendor-authorized, in-person trainings that NARBHA MIS employees have attended off-site over the past two fiscal years.

Title/Certification	**Brief Description**	**Title of Attendee**
Advanced GroupWise 5.5 Administration	Administration of message transfer and post office agents in a GroupWise messaging system	Network Administrator
Advanced Microsoft Access	In-depth Microsoft Access database design techniques	Programmer/Analyst
Advanced Microsoft FoxPro Database Design	Creation and administration of MS FoxPro enterprise-class databases	Programmer/Analyst
Advanced Novell Netware Administration	Advanced Administration of Novell NetWare servers, tuning and optimization, and deploying advanced features	Network Administrator
Basic Microsoft Access 2000	Introduction to use of MS Access as a low-cost database solution	Programmer/Analyst
Certified Information Systems Security Professional (CISSP)	Non-vendor-specific awareness of security principles from a management perspective	WAN Manager
Certified Novell Engineer Update	Exposure to new feature of newest release of the networking software	Network Administrator

Title/Certification	Brief Description	Title of Attendee
Cisco Certified Design Associate (CCDA)	Designing Cisco Wide Area Networks	WAN Manager
Cisco Certified Design Associate (CCNA)	Administering Cisco Wide Area Networks	WAN Manager
CMHC Advanced AGS	Advanced CMHC Reporting tools design and administration	Programmer/Analyst
CMHC Beginning AGS	Basic CMHC Reporting tools design	Programmer/Analyst
CMHC Billing Design	CMHC Billing forms generators, event retrievals and selections	Programmer/Analyst
CMHC Database Design	CMHC database administration and creation of database and transactional components	Programmer/Analyst
CMHC Financial Design	CMHC Financial package components	Programmer/Analyst
CompTIA A+	Basic PC hardware and software configuration	LAN Specialist
CompTIA Network+	Networking fundamentals	LAN Specialist
GroupWise 5.5 Administration	Administration of user accounts in a GroupWise messaging system	Network Administrator
Intermediate Microsoft Access	Deployment of MS Access database solutions	Programmer/Analyst
Intro to SCO Unix	Introduction to SCO OpenServer, using a shell, familiarization with the file system and administrative interface	Network Administrator
Microsoft Certified System Administrator (MCSA)	Deployment and administration of Microsoft Windows XP Professional and Windows 2000 Server	LAN Specialist
Microsoft Database Administration	Basic database design concepts in a Microsoft environment	Programmer/Analyst
Microsoft Visual Studio .Net	Intermediate coding/design strategies for conversion to Visual Studio.net	Senior Programmer Analyst
Microsoft Visual Studio .Net	Intermediate coding/design strategies for conversion to Visual Studio.net	Programmer analyst
Microsoft Visual Studio .Net	Intermediate coding/design strategies for conversion to Visual Studio.net	MIS Director
Novell Netware Administration	Administration of Novell NetWare user accounts, printing, and logical mappings.	Network Administrator
SANS Firewalls, VPNs, and Perimeter Security	Detailed network security class for perimeter network security and defense-in-depth	WAN Manager
SCO Unix Administration I	Administration of SCO OpenServer and UnixWare, scripting intro, shell environments, operating system tuning and optimizing	Network Administrator
WEDI HIPAA Regulations	Implementing programs within HIPAA guidelines	Programmer/Analyst

In conjunction with vendor-authorized training, technical conferences provide a cost-effective mechanism for advanced training. Over the past four fiscal years, MIS staff have attended Comdex, Microsoft FoxPro DevCon, CMHC National Users Group, Microsoft Windows Security Workshop, FBI Information Security conferences, and HIPAA Security/Privacy conferences, to name a few. Usually, conference attendees can pick from a variety of topic-specific didactic training opportunities, as well as networking with other information technology professionals to discover solutions to specific, complex problems.

In the event that the operations of NARBHA or its providers are disrupted for any reason, the NARBHA Leadership Council is responsible for assessing the situation, developing a plan for recovery, coordinating the plan, and communicating the plan to all stakeholders, including members that are affected. The overarching document to guide these activities is the Business Continuity Plan (BCP). The BCP includes a reference for the Emergency Preparedness Plan (EPP) and references a separate Disaster Recovery Plan that is maintained by the Management Information System (MIS) Department for recovery of NARBHA's MIS capabilities. The contract between NARBHA and ADHS/DBHS also is key to the BCP.

As a part of reviewing NARBHA's BCP and related documents, it is important to understand that NARBHA does not provide any direct services to members and serves only in an administrative capacity. NARBHA's system is designed so that its Service Area Agencies (SAAs) and Tribal Area Agencies (TAAs) provide the front-end enrollment, eligibility, and assessment services. On-going treatment services are provided by the SAAs and TAAs, as well as by NARBHA-contracted fee for service (FFS) providers and single case agreement (SCA) providers. Thus, any interruption in NARBHA's operations will not impact service to members. This decentralization allows NARBHA to approach planning for a disaster and recovery differently from an organization that provides direct member services on site.

System Data Archive and Retrieval System

The decentralized member services model provides a built-in member-data redundancy with member enrollment and service data recorded at provider sites, as well as seamless continuity of member services in the event of a disaster affecting NARBHA's headquarters. With this in mind, NARBHA has instituted several procedures and processes that support disaster planning and recovery for NARBHA headquarters and the information systems housed there.

Data backups and archiving

To preserve the information NARBHA needs to support its clinical and administrative business areas, NARBHA provides for regular backups of the data on its critical systems. NARBHA employs two backup software packages, one for the UNIX-based server "CMHCHOST" and the second for all other systems.

1. Cactus Software's LoneTar 4.1 is used for server "CMHCHOST." This is a UNIX-based product that allows for backup of all data, with internal logging of files backed up and an emergency restore/recovery process, Rescue Ranger Disaster Recovery Agent, which allows for an extremely fast restore/recovery process to either an existing or new hardware platform.

2. Computer Associates ARCServe 9.01 for NetWare with Disaster Recovery is a Novell-based product installed on the server "OK," responsible for backing up all other systems. ARCServe has internal logging of files backed up and an emergency restore/recovery process with a disaster recovery option that allows for an extremely fast restore/recovery process to either an existing or new hardware platform.

Both processes noted above allow for a "fast disaster recovery" process that affords the ability to restore a system very quickly. The technology allows a current, or brand new server to be loaded using a disaster recovery diskette to boot the server and access the backup tape/media and restore the entire operating system, drivers, software package, and data, with little or no operator/administrator interaction. This cuts down enormously on the time necessary to reconfigure for a new system, re-install operating systems, configure drivers, install packaged software, and then re-install data. This technology is key to systems recovery in a disaster.

Backup processes, which are run according to the daily, weekly, and monthly schedule below, are run late in the evening of the business day. The backup processes prepare completion logs that are reviewed at the beginning of the next business day by the Network Administrator or designee to determine the success or failure status of these backups. In the event that any server or central computer system backup fails, the Wide Area Network (WAN) Manager decides whether to schedule another backup at the earliest opportunity or to defer it until the following backup cycle. This decision is based on how critical the server is, the impact to the company, and whether there is another method to ensure that NARBHA has the ability to recover critical data. As an example, the WAN Manager may:

- Choose to defer a backup if the Internet/e-mail server ("GWGATE") backup fails, because that system hosts no data and only provides e-mail services

- Defer a backup of the CMHC server knowing that the critical databases are copied to other portions of that system nightly

- Choose to back up the file/print server "OK" because all staff depend on current data stored there

If the WAN Manager defers a backup one day, and the same failure occurs the next business day, he immediately notifies staff and reschedules the backup. The WAN Manager also immediately looks at the failure to determine the cause (hardware, software, scheduling, or media) and initiates corrective actions.

NARBHA employs three types of backups.

- Daily backups occur the evening of every weekly business day and are labeled Monday, Tuesday, Wednesday, and Thursday. These backups are differential, meaning they back up all data that have been changed since the last full backup (weekly or monthly). That is, if the weekly backup is run Friday, then Monday's tape copies changes that occurred between the Friday backup and the Monday backup. Tuesday's tape copies all of what Monday's tape copied, in addition to all changes that occurred on Tuesday. This redundant backup method protects against a bad backup tape and allows NARBHA staff to reload data onto new servers quickly since they can use the latest daily backup tape alone instead of needing multiple daily backup tapes. These daily tapes/media are stored on-site in fireproof file safes to preserve them against damage. The Network Administrator or designee moves the daily tapes to the fireproof safe the next business day once the daily backup has been verified.

- Weekly backups are run every business Friday. Weekly backups are labeled as the 1st, 2nd, 3rd, 4th and 5th Friday of the month. These weekly tapes/media are stored off-site in fireproof file safes to preserve them against damage. The Network Administrator or designee moves the weekly tapes to the off-site fireproof safe the next business day after the weekly backup has been verified.

- Monthly backups are run the last business day of the month and are labeled for the month they contain. These tapes are on permanent retention and are never used again (the daily and weekly backup tapes are reused). These monthly tapes/media are stored off-site in fireproof file safes to preserve them against damage. The Network Administrator, or designee, moves the monthly tapes to the fireproof safe the next business day after the backup has been verified.

The off-site storage area is a facility near the NARBHA Flagstaff headquarters that meets local city codes regarding fire protection and drainage. Access to the facility is by key code from the street, limiting public access to the main site. Interior doors provide extra access control, and the final door is secured with a NARBHA lock. Inside the final storage area NARBHA maintains three fireproof safes, all secured after use. Combinations and/or locks are changed as necessary by the Network Administrator or designee, and as determined by the MIS Director, the Wide Area Network (WAN) Manager, and/or the Network Administrator.

Data Retrieval Testing

To test the efficacy of the tape backup process and the adequacy of the tapes, a set of tapes from each of the weekly and monthly tape backup rotations is selected at random and used to restore a single file to a given server. This restore process is applied to a test portion of the system so as to not impact any production data. If a given set of tapes fail:

- The restore is attempted again to see if it is successful.

- On a second failure:
  - Backup logs are reviewed to see if a message was returned that indicated media is suspect.
  - Tape media are inspected to see if it is necessary to erase the data and destroy the tape.
  - Backup hardware is inspected.
  - Physical hard drives are reviewed to see if there is a problem.

- The backup is rerun as necessary.

MIS Disaster Recovery Plan

NARBHA has prepared policies and procedures to support the return to service of the technical environment in as short a time as practicable. This amount of time would be determined by the size of the disaster—whether it is a single server failure or the loss of the entire NARBHA headquarters facility. NARBHA's current Disaster Recovery Plan is predicated on the following key assumptions and actions.

- NARHBA has defined a cold site suitable to allow installation of the appropriate servers, printers, and personal computers to allow NARBHA headquarters personnel to function. A cold site is an alternate site that can be used to install replacement hardware, software and telecommunications.

- Whenever purchasing server-class hardware, NARBHA chooses equipment that can support the three main operating systems it uses: Novell, Santa Cruz Operation/UNIX, and Windows 2000/Server Edition.

- NARBHA has built strong relationships with account representatives at its major vendors (Dell, COMPAQ, Cisco, etc.) to enhance their understanding of and exposure to NARBHA's business and information systems infrastructure needs, so that NARBHA can solicit the vendors' immediate assistance during the initial phases of disaster recovery.

- All major hardware vendors have committed to be able to replace equipment in a reasonable time frame to allow NARBHA to re-constitute its systems. In addition, major hardware vendors are geographically located outside of Flagstaff, so that a disaster affecting NARBHA is not likely to affect their ability to provide equipment promptly.

- NARBHA has a 36-month replacement cycle for information systems equipment. As server-class machines are removed from service, all Protected Health Information (PHI) is removed and they are stored off-site in such a manner that they can be used immediately as interim servers until actual replacements are received. In addition, personal computers and other equipment, when removed from service, are cleared of all PHI and stored off site in such a manner that they can be used in the interim until actual replacements are received.

- All data are backed up according to NARBHA backup tape rotation policies and procedures as discussed above.

- Upon the declaration of a disaster, after the determination of the scope of the disaster and with the approval of the NARBHA Safety Officer, the Wide Area Network (WAN) Manager will immediately execute the necessary steps to purchase the replacement equipment.

- NARBHA can, through the Internet from any remote personal computer and phone line, effect communication to the provider network to exchange the data files necessary to allow the SAAs/TAAs to do business.

- NARBHA staff will courier information considered critical for performance under the ADHS/DBHS contract. At a minimum, this information will include:
  - Enrollment information (HIPAA/834)
  - Claims/Institutional (HIPAA/837I)
  - Claims/Professional (HIPAA/837PI)
  - Medication Claims (NCPDP)
  - ADHS Demographic (ADHS/Demographic)
  - Quarterly/monthly files necessary to satisfy contract requirements

Based on the backup and retrieval procedures described above, NARBHA can:

- Within 72 hours field an interim data center that can address the specific needs of a NARBHA-based managed care organization

- Within five business days from establishment of the interim data center, reestablish communication between NARBHA and the SAAs/TAAs

- Within 10 business days after establishing communication with the SAAs/TAAs, reestablish communication with ADHS/DBHS

At the time of the disaster NARBHA will immediately contact its insurance carrier to begin the process of claim recovery to pay for destroyed property. Current equipment lists are maintained for this purpose; revised as equipment is purchased, upgraded, and replaced; and filed with NARBHA's insurance carrier.

In the event of a declared disaster, NARBHA will take all precautions to ensure that there is no breach of the confidentiality/privacy policies concerning hard copy or electronic PHI. These precautions include, but are not limited to:

- Physical inspection of the disaster site(s) by the MIS Director or designee to see that no member data is at risk for disclosure

- Physical inspection of the disaster site(s) to determine the physical condition of the fire safes containing backup media

- Security at the affected site(s) to ensure that no looting occurs

- Encryption of all data to be exchanged

- Implementation of other security processes concerning workstations/system access (user ID, password, virus scanning, etc.) and physical security (badges, access control, etc.) at the time the alternate site is implemented

HIPAA Compliance

As part of NARBHA's responsibilities as a covered entity under the security regulations under the Health Insurance Portability and Accountability Act (HIPAA), NARBHA has been reviewing its existing security features and MIS Disaster Recovery Plan components over the last 12 months. Upon completion of a security review tool, HIPAA EarlyView, which is a security review tool from the North Carolina Health Care Information and Communications Alliance, NARBHA will update its MIS Disaster Recovery Plan to be in compliance with the HIPAA requirements by March 2005.

Ongoing Provider Support and Communication with ADHS/DBHS

Because NARBHA relies solely on its provider network for member services, if a disaster occurred that was sufficient to halt NARBHA's ability to function, member services would not be impacted. Key functions would continue as follows.

- Member enrollment/closure functions would not be affected because members would still present to the SAA/TAA intake sites for enrollment. Agencies enrolling/closing members would archive the information until NARBHA was up and running and able to accept it.

- Member demographic functions would not be affected because members would still be enrolled at the SAA/TAA sites. Agencies performing this function and capturing this information would archive the information until NARBHA was up and running and able to accept it.

- Member services are all delivered through subcontracted agencies, not through NARBHA. Agencies would continue to serve the members, archiving claims and encounters until NARBHA was able to process their claims/encounters.

- Payments to SAA/TAA providers could, at the discretion of the Finance Department and Chief Executive Officer, be advanced to the SAAs/TAAs via bank transfer.

- Payments to other providers could, at the discretion of the Finance Department and Chief Executive Officer, continue to be advanced to the FFS/SCA providers via bank transfer.

- Members requiring crisis response could continue to rely on NARBHA's crisis response system comprised of the SAAs/TAAs and ProtoCall, which is a 1-800 telephonic crisis provider staffed with appropriately credentialed professionals.

- Reporting to/from ADHS/DBHS would be affected, but manual transfer of information via courier could be instituted if the lapse in service exceeded a specific time period.

Testing of the MIS Disaster Recovery Plan

NARBHA has tested components of its MIS Disaster Recovery Plan over the past 24 to 36 months.

- Server recovery/data recovery: As an exercise, NARBHA MIS staff have implemented a new, replacement server using the "fast disaster recovery" process. This includes rapid setup, installation, configuration, and restoration of the appropriate information using the disaster recovery processes and the tape backup software described above.

- Interoperability/operational considerations: In one instance, a mission-critical server, Server "CMHCHOST," went off-line due to a component failure. NARBHA MIS staff removed that same component from another, less critical, server and installed it into server "CMHCHOST" to preserve clinical operations at NARBHA. The process was successful in that Server "CMHCHOST" was returned to service with minimal downtime, and the affected component was received the next business day and replaced in "CMHCHOST" with no impact on production.

- Operational considerations: In 2002, one of NARBHA's three Flagstaff office buildings suffered a flood that caused the entire building to be evacuated, affecting the Clinical Operations Department. Affected staff were moved to offices in the remaining NARHBA buildings based on the criticality of their function as defined in the Emergency Preparedness Plan. This plan was in effect for 10 days. During the emergency, NARBHA's Safety Officer visited the affected site regularly to ensure that there was no breach of confidentiality/privacy policies concerning hard copy or electronic PHI.

Business Continuity Plan

In the event that the business of NARBHA or its key providers is disrupted, the BCP is invoked and the NARBHA Leadership Council is convened to the maximum extent possible in the circumstances. The Chief Executive Officer of NARBHA, with assistance from available members of senior management, is responsible for the assembly of the Leadership Council, which assesses the situation and develops an action plan with the goals of:

1) Eliminating or reducing the potential for injuries or loss of human life

2) Stabilizing the effects of the situation, including emergency evacuation and notification to public emergency services agencies

3) Minimizing disruption of services to members

4) Protecting clinical and company information

5) Eliminating or reducing damage to facilities

6) Minimizing financial loss

Consultants are utilized if necessary to make this initial assessment and develop the action plan. The plan may have to be modified as recovery begins and proceeds. For example, if the initial assessment does not identify that an affected building is unusable, the plan has to be modified to arrange for an alternate site. The Leadership Council designates a single point of contact who is responsible for contacting affected members, stakeholders, and the media if appropriate. The Leadership Council may designate Functional Area Recovery Management (FARM) teams to address specific areas of the recovery. If the recovery involves emergencies addressed in the EPP, then that plan is invoked. If the recovery involves an event planned for in the MIS Disaster Recovery Plan, then that plan is invoked. Once business operations are restored, a long term plan is developed for replace of any temporary functions, space or equipment. Events related to the recovery are monitored against the terms of the ADHS/DBHS contract. Finally, and a meeting is held to debrief and learn from the event.

Emergency Preparedness Plan

For development of the EPP, NARBHA takes an “all hazards” approach to disaster planning by reviewing, analyzing, and addressing any and all possible hazards that it determines to be credible and serious threats to the community. NARBHA’s EPP addresses four specific phases of disaster management: mitigation, preparedness, response, and recovery.

- Mitigation activities lessen the severity and impact of a potential emergency. They include identifying potential emergencies that may affect the organization’s operations or the demand for its services, and implementing a strategy that supports the perceived areas of vulnerability within the organization. Some mitigation activities are:
  - Hazard Vulnerability Analysis, a tool the NARBHA Leadership Council completes as necessary, but at least annually, to define and drive mitigation activities for those threats defined as critical.
  - Regular safety inspections of NARBHA’s main site
  - Emergency fire drills
  - Connection of all electrical equipment to electrical surge protection and backup power devices

- Preparedness activities build organization capacity to manage the effects of emergencies, based on the reporting of an emergency and staff notification. Staff members who are concerned about a risk factor are expected to communicate it to those around them, their supervisor, and/or the NARBHA Safety Officer.

- Response activities control the negative effects of emergency situations, through the actions affected staff and management must take when confronted by an emergency.

- Recovery actions begin almost concurrently with response activities and are directed at restoring essential services and resuming normal operations. Recovery actions may require large amounts of resources and time. A key component of recovery actions is the steps necessary to resume normal business operations.

NARBHA’s major providers, the SAAs/TAAs, also have business continuity/emergency preparedness plans.

Testing of the Business Continuity Plan

NARBHA’s Leadership Council modifies, reviews, and approves the BCP at least annually, and it is reviewed throughout the year as events occur that could cause the plan to be implemented. As these occur the Business Manager may make changes to the plan and re-submit it to the Leadership Council for approval. The BCP also undergoes evaluation each time it are used, to allow participants to evaluate how the process went and what changes are necessary or desirable.

Examples of testing of the BCP include:

- After the massive fires in the White Mountains of Eastern Arizona in 2002, NARBHA reviewed its EPP using input from the affected SAAs, Community Counseling Centers and Little Colorado Behavioral Health Centers. NARBHA amended its Hazard Vulnerability Analysis to consider that the risk of wildfire is higher than was planned for earlier, changes were made to the implementation steps, and the EPP was reviewed and re-approved. Procedures that were implemented to respond to the fire and associated evacuation included:
  - Members being treated at a Level I sub-acute facility were relocated
  - SAA staff were relocated to other sites to provide member services
  - Extensive radio advertising was put into place to reach members and provide a phone number for reaching the SAA that was in the evacuation area.
  - All paper records were moved to a Holbrook provider site, which was outside the fire zone
  - Additional resources from throughout the state were accessed to replace capacity.
  - The provider network was temporarily expanded to include additional prescribers, such as general practitioners, as a means of ensuring access to medical services.
  - Data entry was completed at the main provider site, which was 50 miles away and outside the fire zone.

- In 2002, a NARBHA headquarters building suffered a flood that caused the entire building to be evacuated, affecting the Clinical Operations Department. The Safety Officer implemented components of the EPP that dealt with communications and critical functions. Affected staff were moved to available offices in the remaining two

NARBHA buildings based on how critical their function is as defined in the EPP. This emergency plan was in effect for 10 days. At the post mortem, NARBHA leadership recognized that a safety issue not addressed prior to staff re-entry into the building was levels of mold/spores encountered by staff returning to the evacuated offices. Although once mold testing was completed and no problems found, the EPP was updated to including this type of testing in the future.

- In July 2003, NARBHA moved its company headquarters from three separate offices to a single Flagstaff building. Components of the plan dealing with availability of key functions were used to ensure that the member representative function was in place and functioning with technology and phones at all times.

NARBHA ensures confidentiality, integrity, and availability of all electronic information created, received, maintained, and transmitted by the organization. NARBHA's Management Information Systems Department (MIS) approaches information systems security following best practices as outlined by the International Information System Security Consortium (ISC2). ISC2 is a global, non-profit organization consisting of information systems security professionals, which has established a non-vendor-specific Common Body of Knowledge (CBK) that has been adopted as the standard worldwide. The CBK is divided into 10 major categories, or "domains," each of which is addressed below individually as it relates to NARBHA's security practices. In addition to the 10 domains of the CBK, NARBHA's handling of audit trails and logging is discussed in detail in this section.

Domain 1: Security Management Practices

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines regarding those assets.

As a behavioral health managed care organization, NARBHA is complying with the Heath Information Portability and Accountability Act (HIPAA). NARBHA has outlined its process for security management (NARBHA Internal Policy 1504, Security Management), which encompasses information systems security as well as other areas such as physical security. New employees are informed of NARBHA security standards before conducting business; therefore new employee orientation takes place in a timely manner (NARBHA Internal Policy 5501, Employee Orientation Policy). New employees are provided a general overview of NARBHA's security management strategy, as well as instructions on how to handle Protected Health Information (PHI) responsibly (NARBHA Internal Policy 7502, Use and Disclosure of PHI). New employees also are expected to read and sign a Software Code of Ethics (NARBHA Internal Policy 4402, Software Control Policy, Attachment A), which outlines the ethical and permitted use of software during employment at NARBHA. Additionally, all employees are initially and periodically screened to ensure that they are qualified to responsibly and securely manage information in their respective area of expertise (NARBHA Internal Policy 5102, Performance and Competency Assessment, Review of Credentials).

NARBHA requires all outside entities that will have access to Protected Health Information to adhere to a baseline standard of non-disclosure under a HIPAA-compliant business associate contract (NARBHA Internal Policy 2104, Business Associates—HIPAA Use and Disclosures). NARBHA mandates secure interactions adhering to the HIPAA standards with NARBHA Service Area Agencies (SAAs), Tribal Area Agencies (TAAs), and fee for service (FFS) and single case agreement (SCA) providers for electronic submission of claims data (NARBHA Internal Policy 2514, Privacy of Claims and Claims Information). NARBHA also outlines the process by which it submits encounter data securely to ADHS (NARBHA Internal Policy 2522, Encounter Submission). This process is discussed in detail in Volume 5.k.

Domain 2: Security Architecture and Models

The security architecture and models domain contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, and applications, as well as those controls used to enforce various levels of availability, integrity, and confidentiality.

NARBHA designs its Wide Area Network (WAN) and Local Area Network (LAN) security architectures by employing multiple technologies to establish defense in depth and maintains a consistent level of information security across the network. NARBHA uses open systems, or systems that use standard interfaces and interoperate with other vendor systems, for WAN and LAN hardware, server and PC hardware, network operating systems, and standard application software. NARBHA does not employ proprietary or closed systems in its information systems environment because closed systems may not interact well with open systems.

Any network that is not within NARBHA's span of direct control is considered untrusted. NARBHA employs network partitioning at all points of interface to untrusted networks, the largest untrusted network being the Internet. NARBHA implements network partitioning through a combination of security technologies that perform packet filtering, stateful inspections, proxy services, virus scanning, and access control.

NARBHA does not use wireless LAN technologies, the most compelling reason being the resultant "de-perimeterization" of the network. Due to the nature of a wireless signal, there are no clearly delineated "edges" to the network. Signals may be easily intercepted from outside the physical structure, using readily available tools such as wireless “sniffers.” Security protocols designed specifically for wireless technologies have been found to be flawed. Even the most secure wireless LANs are not 100% safe.

Standardization is another important element in NARBHA’s security architecture. NARBHA deploys PCs with standardized hardware as well as a standard software build of tier 1 applications. NARBHA MIS applies all upgrades/patches to servers in such a manner that all like servers are at the same revision level, and tests patches prior to implementation in the production environment. Finally, NARBHA MIS disables or unloads unused protocols (IPX, NetBUI, NFS, TFTP, and SNMP) on all hosts and devices.

New employees are oriented in NARBHA’s standard security practices, which are outlined in NARBHA’s policies and procedures. Major topics include: responsible and secure e-mail use, secure password practices, desktop security and screen locks, proper file storage procedures, introduction of removable media to the protected network, and virus prevention and detection. Existing employees are periodically updated and reminded of NARBHA’s security standards at monthly all-staff meetings, and are alerted to any changes. Additionally, mandatory training on HIPAA guidelines is routinely performed for all employees.

Domain 3: Access Control Systems and Methodology

Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

NARBHA MIS provides access control to all electronic information-based systems on a need-to-know basis only (NARBHA Internal Policy 4201, Systems Security Access Control); this process begins with an electronic System Change Request by an employee’s supervisor (NARBHA Internal Policy 4306, Systems Change Request). This process provides an electronic audit trail for when access was requested, what type of access was granted, and when and for whom access was granted.

NARBHA’s Network Administrator or designee provides initial passwords to new employees (NARBHA Internal Policy 4204, Data Security). Users are oriented on password best practices and are required to enforce minimum password standards. MIS performs a password audit as necessary using LØphtCrack/LC4 for Windows. Users with weak passwords are reoriented on password security and are expected to change their passwords immediately.

Access control to multiple servers is handled through Novell *e*Directory authentication. *e*Directory is a distributed directory database that is fully replicated among multiple servers at NARBHA, and is arguably the most mature and sophisticated directory service available today. Within *e*Directory, specific access permissions are assigned for a particular job function through an Organizational Role Object. New user accounts for employees are created after completion and approval of a System Change Request. New users are subsequently linked to the Organizational Role Object that corresponds to the position they are hired for, thereby providing access to the minimum necessary applications and folders required to perform their duties, and no others. This process ensures access control consistency from one employee to the next in the event of staff turnover.

Through Novell ZENworks and Novell Application launcher, NARBHA MIS “pushes” mission-specific applications to users regardless of the workstation they are using. Through *e*Directory, Novell ZENworks, and Novell GroupWise, users can log on to any PC on the LAN and securely access all appropriate resources while being provided the same look and feel of their own PCs. NARBHA Help Desk professionals also use Novell ZENworks to remotely control a user’s PC to resolve software-related problems, regardless of which PC the user is using.

NARBHA’s most mission-critical system, CMHC/MIS, employs two independent layers of access control. The first layer is the Santa Cruz Operation (SCO) UNIX operating system User ID, which controls the software, files, and operating system commands a user is allowed to access. The second layer is built into the CMHC/MIS system. A unique CMHC/MIS sign-on ID is issued and is synchronized with the corresponding UNIX User ID. Administrative tools allow NARBHA MIS to control which menus, functions, and even data elements a user can access within the suite of CMHC/MIS software components based on their need to know and User ID.

NARBHA MIS staff also manages the process to obtain passwords that are required to access or contribute data to external databases, such as those that are operated by ADHS/DBHS, which are needed as a part of NARBHA’s operations (NARBHA Internal Policy 4613, Contribution and Access to External Databases). A NARBHA user submits a System Change Request to request access to an external resource, and then NARBHA MIS makes a formal request for access to the external entity on behalf of the requesting user by submitting the appropriate documentation.

Access control history information is tracked through system logging, which is captured and reviewed either weekly or daily, depending on the device that is reporting. Detained information of system auditing and logging is discussed in the "Audit Trails and Logging" portion of this section.

Domain 4: Application Development Security

This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

NARBHA MIS standardizes in-house development and programming processes through the NARBHA Programming Standards and Guidelines, a document that outlines where production programs and test/development systems are to be located within the file structures of each host. Programming personnel are granted exclusive access to development file structures. Additionally, standardized directory layouts, specific file naming conventions, and supporting documentation of written code ensure consistency. Change management is maintained through this supporting documentation.

To simplify the environment for end-users, the NARBHA Programming Standards and Guidelines specifically address a standard look and feel for the user interface, as well as consistent formatting guidelines for the generation of internal and external reports prepared by MIS. In addition, NARBHA embraces Object Oriented Programming because of the security aspect of self-contained objects as opposed to lines of code, as well as the efficiency of reusing blocks of code.

NARBHA MIS thoroughly tests new or modified software deployments internally on all operating system platforms that will be supported by the software. MIS staff reviews end-user documentation to ensure that the instructions for installation or use are consistent with the documentation provided. Once MIS staff have performed rigorous software testing, a cutover date is specified and disseminated.

Domain 5: Operations Security

Operations security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report pertinent information to the appropriate individual, group, or process.

The goal of NARBHA's operational security strategy is to protect information system resources. NARBHA MIS achieves this by identifying NARBHA's resources (i.e., PHI, hardware, software, source code, licensed software, and auxiliary storage media), and the types of threats that may be encountered (e.g., disclosure, destruction, corruption, theft/removal). As a part of NARBHA's HIPAA security compliance efforts, MIS security associates are performing an ongoing security gap analysis by using the North Carolina Health Care Information and Communications Alliance HIPAA EarlyView Security assessment tool. This software tool covers many aspects of security and facilitates in-depth self-analysis pertaining to information systems security. As part of this gap analysis, security deficiencies have been identified and addressed. This process has protected NARBHA's MIS environment from information systems security emergencies, such as worms and viruses, which have plagued many companies to date.

NARBHA's MIS Director or designee conducts continuing education and awareness training and continually monitors users for security compliance during day-to-day operations such as electronic messaging (NARBHA Internal Policy 4205, E-Mail Usage). Employees are not allowed to utilize personal hardware or software in the workplace unless such use will enhance the employee's productivity, for instance, through installation of interface software or a carriage for a Personal Data Assistant. Employees must formally request to use their personal hardware and/or software at NARBHA, and the request is scrutinized by NARBHA MIS for potential security vulnerabilities. If the request is approved, the change is implemented by MIS network professionals (NARBHA Internal Policies 4401, Personal Software Policy and 4404, Personal Hardware Policy) to ensure proper functioning of the addition in the NARBHA PC environment.

NARBHA appropriately treats software as a valuable resource, maintaining appropriate numbers of licenses in accordance with what is actually used. NARBHA's Network Administrator and Business Manager tightly maintain software licenses (NARBHA Internal Policy 2113, Software Licensing). Software may not be taken or duplicated by any NARBHA employee when copyright conditions apply (NARBHA Internal Policy 4402, Software Control Policy).

Each workstation and server in the NARBHA network runs current antivirus software that is updated nightly. In addition, server software scans all files that users access or copy to mass disk storage. Any device or file found infected with a virus is quarantined, cleaned, and then reintroduced to the protected network (NARBHA Internal Policy 4403, Computer Software Virus Checking-Removal).

NARBHA takes extra security precautions with laptop computers. The standard laptop hardware configuration requires any integrated wireless network controllers to be disabled in BIOS settings; this configuration also contains a ZoneLabs ZoneAlarm personal firewall, SpyBot Search & Destroy anti-spyware software, and Lavasoft Ad-aware anti-adware software. Users are trained in proper secure laptop use (NARBHA Internal Policy 2114, Use of NARBHA Laptop Computers) before they are authorized to check a laptop out of the corporate laptop pool. Mobile users are not authorized to add, remove, or modify the standard software build without written approval from the Network Administrator. (NARBHA Internal Policies 4401, Personal Software Policy and 4404, Personal Hardware Policy).

As a HIPAA covered entity, NARBHA is responsible for maintaining strict confidentiality of PHI (NARBHA Internal Policy 7304, Maintaining Security of Member Information). Additionally, computer screens are safeguarded when an employee is away from his or her work area through a requirement that employees initiate their screensavers every time they step away from their workspaces. Each screensaver is password protected (NARBHA Internal Policy 4204, Data Security) and, as a backup, set to automatically initiate after five minutes of inactivity.

NARBHA employees are routinely reminded of verification procedures to mitigate a potential security violation from "scams" such as phone calls where someone poses as a fellow employee with an urgent problem.

Employees who are terminated, whether voluntary or involuntary, are required to return all NARBHA equipment, including any PCs or laptops (NARBHA Internal Policy 5714, Termination of Employment) in the original condition in which the equipment was provided. Access to information systems resources is removed through the supervisor's submission of a Systems Change Request. If the termination is involuntary, access to information systems is immediately removed through an e-mailed request by the supervisor, who subsequently submits a Systems Change Request. With resignations, access to information system resources is removed based on the employee's termination date.

Domain 6: Physical Security

The physical security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

Physical security is an important aspect of information systems security. NARBHA employs a layered defense model, meaning security measures increase as one enters deeper into the corporate headquarters building.

Starting with the perimeter and building grounds, landscaping is performed so that branches of trees are trimmed to be at least six feet from the ground and bushes are groomed to grow less than two feet tall. Structural barriers allow only foot-traffic entry into the building. Lighting on the outside of the premises automatically illuminates outside areas, beginning at dusk each evening.

The building itself is safeguarded with an alarm system. Employees enter the building using a Simplex card key lock system with tiered access control within different parts of the building. Successful entry is logged to a database within the server-based card key lock system. The database shows an alarm if any keyed door is left open for more than 20 seconds.

Only one exterior door is unlocked during business hours. This door enters into the receptionist area, which is always staffed during business hours. Entrance from the reception area to the rest of the building is by key card only. All visitors are required to sign in and out, must wear numbered visitor badges, and must be escorted at all times by a

NARBHA staff member (NARBHA Internal Policy 1504, Security Management). In addition, NARBHA staff members are required to wear their picture IDs at all times. All other exterior doorways are dependent on a valid card key to enter. The only windows in the building that can be opened are located on the second floor. For safety purposes, local law enforcement members have been familiarized with the physical layout of the building, while six hand-held radios are routinely monitored from strategic locations within the building to ensure immediate response in the event of emergences. Additionally, fire prevention, detection, and suppression safeguards protect NARBHA employees, visitors, and physical assets.

NARBHA's secure data center is located at the core of the corporate building and requires a Simplex key card with specific permissions to enter (see Diagram 5.a.1 below). Only select MIS, Telemedicine, and Security staff have access to the data center. The data center has its own air-conditioning units. There are two backup air conditioning units in case of a failure of the main DataAire unit, which services both the temperature and humidity requirements of the data center. The data center also features a false floor, independent electrical facilities, and an Ansul Inergen waterless fire suppression system. Inergen suppressive gas consists of a mixture of nitrogen, argon, and carbon dioxide that will not harm electronic components within the data center. All components of the data center adhere to the ANSI/TIA/EIA-569-A Standard for Telecommunications Pathways and Spaces. The data center is populated with mission-critical telecommunications, data, video, and voice equipment. All equipment is connected to uninterruptible power supplies that provide "clean" power and protects against complete or partial power system failures.

Temperature, humidity, and dew point in the data center are monitored by Ethernet-enabled Newport iServer MicroServer (Firmware 2.1) sensors. These devices are located in each of the Intermediate Distribution Facilities as well as the Main Distribution Facility in the data center. Sampling every 20 seconds allows for web-based charting to determine trends. E-mail alarms notify data network professionals any time thresholds are exceeded.

All information systems equipment or hardware is tagged with a NARBHA Property Control Tag within one month of deployment. Property control logs are maintained by the Business Manager and are inventoried annually for accuracy (NARBHA internal Policy 2101-Physical Control of Assets). This process allows NARBHA to account for all of its resources.

Domain 7: Cryptography

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

NARBHA provides its own Public Key Infrastructure (PKI) for encryption for internal uses such as secure web-based e-mail. A Microsoft Windows 2000 Advanced Server provides Stand-alone Root Certificate Authority (CA) services, while another Windows 2000 Advanced Server provides Subordinate CA functions. These CA servers are used for enabling secure electronic transactions to NARBHA's Intranet/Extranet web services and secure internal host management. There is a fully redundant certificate repository for this PKI configuration.

NARBHA users can access their enterprise messaging mailboxes remotely through a 128-bit Secure Sockets Layer (SSL) Secure WebAccess interface, providing encryption, authentication, and integrity. Additionally, NARBHA's Intranet and Extranet can only be accessed through SSL, which is a secure interface as opposed to the standard HTTP (Internet) connection.

NARBHA MIS manages robust secure remote connectivity through a Cisco 3005 Virtual Private Network (VPN) Concentrator, allowing for concurrent connections by up to 250 users. Each remote PC connects through the Cisco Universal Client, which features an "'always on" personal stateful firewall, allowing for connections only when using 168-bit 3DES encryption. An MD5 hash algorithm ensures the integrity of encrypted data that are sent over the Internet through the VPN.

Protected Health Information is not authorized on remote PCs, nor may this information be transmitted unencrypted over the Internet (NARBHA Internal Policy 4202, Member Data Over the Internet). Member data that are delivered to ADHS/DBHS are either sent through NARBHA's private, point-to-point connection or encrypted with 128-bit SSL and compressed through PKZIP Professional, then password protected. NARBHA is currently testing Secure File Transfer Protocol (SFTP) transactions using WS-FTP with ADHS/DBHS as well.

Domain 8: Telecommunications, Network, and Internet Security

The telecommunications, network, and Internet security domain discusses network structures, transmission methods, transport formats, and security measures used to provide availability, integrity, and confidentiality.

WAN Topology: The Wide Area Network (WAN) infrastructure consists of a single core site at NARBHA's Flagstaff headquarters, 6 intermediate sites, and 18 edge sites throughout Northern Arizona. Private, point-to-point T1 circuits connect video, voice, and data traffic through static bandwidth allocation. This fiscal year, NARBHA will implement dynamic bandwidth allocation at each location when it moves to an IP-based model for video, voice, and data services. This will greatly enhance bandwidth performance to all remote sites.

Telecommunications hardware consists of a fully redundant DS3 cabinet. The DS3 is a fiber optic line that carries the equivalent of 28 T1 lines. DS3, as opposed to multiple T1s, provides the efficiency of expedited scalability and a significant overall cost savings. The DS3 coming into NARBHA's Flagstaff headquarters is channelized (divided) into 28 T1 (1.544Mbps) circuits by an Adtran MX2800 M13 multiplexer unit with fully redundant processor card. These T1 circuits carry video, data, and voice signals. Approximately 30 analog phone lines provide emergency voice, fax, and modem access in the unlikely event of a DS3 failure. Currently, a NET Promina 800 ISDN Switch and Frame Relay Access Device provides Frame Relay and ISDN switching services, sending data and video signals to the NARBHA core router and videoconferencing bridge. All telecommunications and WAN-related equipment is supported by battery backup and features redundant power supplies.

Perimeter Security: NARBHA provides Internet access to its SAAs through two T1 direct Internet access connections. This allows for 3Mbps of concurrent Internet bandwidth. Full stateful firewalling and virus scanning are performed on all Internet traffic. Stateful packet filtering is employed at each of two Cisco PIX 506e firewalls. Standard and extended access control lists implemented on all routers in the NARBHA data network provide packet-level security.

A virus-scanning and content-filtering McAfee e500 WebShield appliance scans and cleans all inbound and outbound Internet traffic, including e-mail, hypertext, and file transfers. The WebShield appliance also blocks inbound traffic that appears on a regularly updated database of known spam sites or a 'blacklisted' domain name. In the event of "false-positives," MIS staff can manually add domains or sites to a permit list.

Network Management: The ability to safely administer a WAN requires extensive tools for efficiency and auditing purposes. NARBHA currently employs the following tools:

- *GFI LANguard Network Security Scanner* is used to ensure that recent security patches have been deployed on PCs and servers as well as checking network hosts for common vulnerabilities. In FY 2005-2006, NARBHA will deploy Cisco's SecureIDS stateful network intrusion detection system as software code running on the new core router.

- *Ethereal Network Protocol Analyzer* is used to capture network traffic for troubleshooting of communications problems and detection of network anomalies.

- *Cisco ConfigMaker* is used to add or perform upgrades or configuration changes to core, intermediate, and edge Cisco routers within the WAN from a single PC.

- *Foundry Ironview Network Manager* is used to add or perform upgrades or configuration changes to the Foundry FastIron 800 core switch.

- *Dell OpenManage Network Manager* is used to add or perform upgrades or configuration changes to all of the Dell PowerConnect 5224 switches in the LAN.

Domain 9: Business Continuity Planning

The Business Continuity Plan domain addresses the preservation and recovery of business operations in the event of outages.

NARBHA has an Emergency Preparedness Plan (EPP)/Business Continuity Plan that serves as a roadmap in the event unexpected events impact NARBHA's operations. A portion of the EPP relates to the Management Information System

(MIS) Disaster Recovery Plan, which describes procedures to recover data and continue core information system operations in the event of a disaster.

NARBHA's EPP has been in place for several years to support business continuity in the event of an emergency or natural disaster. The EPP is based in part on NARBHA's Hazard Vulnerability Analysis, which allows NARBHA to evaluate potential adverse events based on probability, risk, and preparedness. The NARBHA Business Manager is designated as the Safety Officer and is responsible for all aspects of the EPP. In the event the Safety Officer is not available, the Assistant Safety Officer/Operations Specialist assumes responsibility for implementing the EPP.

The MIS Disaster Recovery Plan and its underlying policies and procedures describe NARHBA's process for data archival and retrieval. To preserve the information NARBHA needs to support its clinical and administrative business areas, NARBHA provides for regular backups of the data on its critical systems. NARBHA employs two backup software packages, one for the UNIX-based server "CMHCHOST" and the second for all other systems. Backup processes are performed according to a daily, weekly, and monthly schedule and are tested regularly to ensure the integrity of the backup data and medium.

NARBHA also has policies and procedures to support the return to service of the technical environment in as short a time as practicable. This amount of time would be determined by the size of the disaster—whether it is a single server failure or the loss of the entire NARBHA headquarters facility. Implementation of the MIS Disaster Recovery Plan will allow NARBHA to field an interim data center within 72 hours, and resume communication with ADHS/DBHS within an additional 15 business days. There are also procedures in place to ensure the confidentiality and security of PHI.

Various components of both the EPP and the MIS Disaster Recovery Plan have been tested over the past two to three years. This has included tests of plan elements, such as implementing a new server using the archived data from the server being replaced, as well as implementing portions of the EPP during massive fires in Eastern Arizona during 2002 when a provider site had to be evacuated and service capacity replaced. Testing and implementation of any portion of NARBHA's EPP or MIS Disaster Recovery Plan results in evaluation and revisions to the plans as needed.

Domain 10: Law, Investigations, and Ethics

The Law, Investigations, and Ethics domain addresses computer crime laws and regulations, and the measures and technologies used to investigate computer crime incidents.

NARBHA provides orientation and training to all employees regarding expectations and requirements concerning privacy and security, along with the consequence of violation of those expectations and requirements. (See NARBHA Internal Policy 5501, Employee Orientation). All NARBHA employees are required to report suspected breaches of privacy and security to their immediate supervisor, who is then required to notify the Privacy Officer or Security Officer (NARBHA Internal Policy 4202, HIPAA Violations). All employees are also expected to read and sign a Software Code of Ethics (NARBHA Internal Policy 4402, Software Control Policy, Attachment A) that outlines ethical use of NARBHA software resources, including awareness of software piracy.

On a broader scale, NARBHA provides education to employees on preventing, detecting, reporting, and investigating *all* forms of fraud and abuse (NARBHA Internal Policies 2802, Prevention and Detection of Fraud and Abuse and 2803, Reporting and Investigating Suspected Fraud and Abuse). Finally, NARBHA MIS monitors for the potential of computer-related crime activity by subscribing to notifications from various watchdog organizations such as the Computer Emergency Response Team (CERT) and BugTraq.

Audit Trails and Logging

Maintaining and reviewing system audit reports allow networking professionals to identify threats from both inside and outside the organization to protect sensitive information. There is no single solution that can interface with all information systems components to provide audit trails and logging, so NARBHA has employed several best-in-class auditing products.

Each of the auditing tools described below generates reports at specific intervals; these are reviewed as noted below by either the WAN Manager or Network Administrator. When unusual activity is detected, the anomaly is immediately reported to the Privacy Officer or Security Officer (NARBHA Internal Policy 4202, HIPAA Violations), then the event is thoroughly investigated. The report is retained for legal and historical purposes. Data network and/or programming staff, as appropriate, investigate the anomaly to determine whether it is caused by intentional access violation or system corruption. If there is evidence of intentional breach of security, immediate security countermeasures are taken through security device reconfiguration, data packet collection, and, as a last resort, disconnection from the public Internet.

SCO UNIX-SCOadmin Audit Manager

The SCOadmin Audit Manager uses the built-in audit subsystem to track all activity within the operating system. While the audit subsystem can provide accounting for numerous system events, NARBHA tracks only those of high security concern. This minimizes the impact of auditing on overall system performance and generates a more comprehensive and concise report. Events that are audited weekly by NARBHA through the SCOadmin Audit Manager are:

- Admin/Operator Actions
- Login/Logoff
- Object Create/Modify
- Process Create/Delete/Modify
- Resource Denials
- Startup/Shutdown

While the SCOadmin Audit Manager generates reports weekly, templates can be created to collect more detailed information regarding activities of a specific user or group on an ad hoc basis. An MIS staff member is responsible for reviewing the report weekly and reporting any discrepancies.

CMHC DBAudit

In addition to the SCOadmin Audit Manager, the CMHC/MIS database system possesses its own logging and auditing component called DBAudit. This component tracks all or select CMHC databases and can log specific functions within databases such as:

- Display fields
- Change/Update fields
- Add/Remove fields

DBAudit reports the date, time, owner, process, and fields being affected for every register (or primary key within the database) from which it is configured to collect information. DBAudit tracking can be isolated to specific areas within the large database, such as collecting information on removals of client data, or logging changes in payroll data and not accounts payable data. Due to the volume of changes in the CMHC database, the resulting growth of the DBAudit log, and the massive system resources required to collect the information, this feature is used when other security monitoring devices indicate suspected infiltration or when investigating database corruption.

Microsoft Windows Server and Novell NetWare BlueLance LT Auditor+ V8.0 SP3

LT Auditor+ provides real-time, customizable, and detailed audit information for a hybrid Windows server and NetWare networking environment. It is centrally managed on one of NARBHA's Windows 2000 Advanced Server hosts and tightly integrates with both Microsoft Active Directory and Novell *e*Directory. Weekly generated reports provide detailed information on five major areas (users, groups, containers, volumes/logical drives, and files) to identify vulnerabilities. Events that are regularly audited by NARBHA through the LT Auditor+ Report Generator are:

- User objects such as security equivalents, log-in information, and trustee assignments
- Group objects such as group members, group security equivalences, and group trustee assignments
- Containers, including intrusion detection settings, trustee assignments, and objects available within the container
- NetWare and Windows volumes and logical drives such as available space and significant use changes
- File information such as owner, size, last modified date, and attributes

Reports created by the Report Generator are reviewed weekly. However, if an anomaly is identified, other telltale information may be captured and the frequency of review increases.

Kiwi SysLog Daemon 6.1.0

Key network hardware such as routers and switches is configured to receive, log, display, and forward information to a system logging (SysLog) server for centralized log inspection. The Kiwi SysLog server resides on one of NARBHA's

Windows 2000 hosts. This log is reviewed each morning, during the same time period that tape backups are verified for completion. The information sent to the SysLog server may vary, based on the sophistication of the network device. Here is the common information captured:

- Authentication information
- Configuration changes
- Exceeding a preset threshold such as data traffic
- Resets
- Password changes
- Management port status changes

NARBHA uses two main data systems to capture, manage, and manipulate all member-level information. The two data systems are implemented such that the strengths of each complement the other. The two systems are the CMHC system and the Visual FoxPro custom applications.

1. **The CMHC/Management Information Systems (MIS) system** is the central repository to track/manage member level information. CMHC/MIS allows NARBHA to efficiently capture and manage information in the following areas:
   - Member enrollment/disenrollment and demographic data capture
   - Eligibility data capture
   - Adjudication of all claims (Institutional/Professional) for all providers whether they are Service Area Agencies (SAAs), Tribal Area Agencies (TAAs), fee-for-service (FFS) providers, or single case agreement (SCA) providers
   - Authorizations for covered FFS claims to specific members
   - Contract information for all providers whether they are SAAs, TAAs, FFS providers, or SCA providers

   CMHC/MIS, as implemented at NARBHA for managed care organization functions, can be easily modified by authorized system administrators as necessary for customized data capture. The SAAs/TAAs that NARBHA subcontracts with to capture enrollment, eligibility, and demographic information are all either using the CMHC/MIS data system or providing hard copy documentation to NARBHA for later data entry by NARBHA into a CMHC system specific to that agency. This common data system approach, achieved through the consistent use of the CMHC/MIS data system, supports a common understanding and use of the data by NARBHA and the SAAs/TAAs, which allows required information to be defined and captured in the same manner.

2. **Visual FoxPro custom programming** allows NARBHA to design systems to capture information that is not related to, or is supplemental to, the information in the CMHC system. These data needs are additional functional requirements that are unique to any managed care organization and typically track information across providers, whether they are NARBHA's SAAs, TAAs, FFS providers, or SCA providers. These systems typically fall within one of the following categories:
   - Additional data capture processes that are not included in CMHC systems and do not lend themselves to that platform
   - Programs/systems that are developed to supplement the CMHC data system in the areas of data transformation, edit checking and validation, and web based applications

Between these data systems, CMHC/MIS and Visual FoxPro custom programming, NARBHA maintains a centralized data dictionary that contains key information on the types of data NARBHA has available at the data element/field level and its various uses. This information, NARBHA's data dictionary, is comprised of information required by its various stakeholders:

- Key data elements/requirements as defined by ADHS/DBHS contract/policy
- Data elements/requirements as defined in the ADHS/DBHS Client Information Systems (CIS) and Layout Manual
- Data elements that are recorded centrally to allow NARBHA's providers to better manage the tasks NARBHA has delegated to them
- Data elements/requirements as defined internally by NARBHA departments that are critical to its business
- Data elements/requirements as set forth in the Health Insurance Portability and Accountability Act (HIPAA)
- Data elements that are submitted to NARBHA by contracted providers, such as pharmacy benefits management by CaremarkPCS

DATA MAPPING

Below are a series of data mapping documents that demonstrate the ability of NARBHA to capture the requisite information and the understanding to create the required data submission transactions defined in this RFP. The data mapping documents include:

- HIPAA 834 (Enrollment and Closure)
- 837I (Institutional Claim)
- 837P (Professional Claim)
- Demographic

- NCPDP (Drug Claim)
- NCPDP (Supplemental)

Diagram Legend

- Data Element Name: Long name of the data element/field as it occurs in NARBHA's data system
- Short Name: Short name associated with the data element/field when referencing it in the associated data system
- Data Type: The type of data element/field, whether numeric, alphabetic, date, etc.
  - D Date
  - I Integer
  - N Numeric
  - R Record Header
  - T Time
  - X Alpha Numeric
- Len: Length of the data element
- Data Field Validation: What validation is supplied to the data element/field. These are typically applied at the time of input/entry into the data system. Data elements/fields can be validated within or outside of CMHC
- Data Field Validation Table: Edits within CMHC are applied using the values included within the data validation table with this number.
- Mapping Reference: This links the data element to the associated field as defined in the file specifications in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004). The actual mapping methods are defined in the section for each transaction.
- Where the Element is used: This is to demonstrate data elements/fields are used in many of the different transactions that ADHS/DBHS has asked NARBHA to map.
  - HIPAA 834 (Enrollment and Closure)
  - 837I (Institutional Claim)
  - 837P (Professional Claim)
  - Demographic
  - NCPDP (Drug Claim)
  - NCPDP (Supplemental)

HIPAA/Enrollment – 834 (Enrollment and Closure)

Below are the data elements NARBHA uses to prepare the *HIPAA 834 Admit and Closure* data submission transaction as defined by the HIPAA-compliant ASC X12N 834 Benefit Enrollment and Maintenance Transaction Format and the Client Information System (CIS) File Layout Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping is to tie the NARHBA data element/field to the associated element in the *HIPAA 834* mapping through the use of the FIELD Identifier (located in the 7th column of the table below). NARBHA mapped the various fields defined in the CIS layout and other standardized fields that should be defined in a HIPAA 834 transaction. This data transaction has been in production at NARBHA since October 14, 2003, and has been reviewed and approved by ADHS/DBHS staff. Since October 15, 2003, this data submission format has been changed, re-tested, and re-approved.

Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	Where the Element is used					
							834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
MCO DISENROLLMENT DATE	$$EN.LAP	D	10	Past Date Warning		2000/DTP01-357	Y					
OLD INTAKE DATE	C.OLD.IDTE	D	10	No CMHC Edit		2000/DTP03	Y					
MCO ENROLLMENT DATE	$$EN.EFF	D	10	No CMHC Edit		2000/DTP03	Y					
RBHA MEMBER ID	C.ID	X	10	No CMHC Edit		2000/REF02	Y					
CIS CLIENT ID	C.AZ.ID	X	10	No CMHC Edit		2000/REF02-0F	Y	Y	Y	Y	Y	Y
AHCCCS ID #	C.ID.S.DMH	X	10	No CMHC Edit		2000/REF02-6O	Y					
BIRTH DATE	C.BD	D	10	Future Date Warning		2100A/DMG02	Y	Y	Y	Y		
SEX	C.SEX	X	1	Data Code Table	022	2100A/DMG03	Y	Y	Y			
MARITAL STATUS	C.MAR	X	1	Data Code Table	282	2100A/DMG04	Y					
ETHNIC CODE	C.RACE	X	2	Data Code Table	160	2100A/DMG05	Y					
PRIMARY LANGUAGE	C.PRILANG	X	2	Data Code Table	118	2100A/LUI02	Y					
ADDRESS (1)	C.ADDR1	X	26	No CMHC Edit		2100A/N301	Y	Y	Y			
ADDRESS (2)	C.ADDR2	X	26	No CMHC Edit		2100A/N302	Y	Y	Y			
CITY-CLIENT	C.CITY	X	20	No CMHC Edit		2100A/N401	Y	Y	Y			
STATE	C.STATE	X	2	Data Code Table	032	2100A/N402	Y	Y	Y			
ZIP CODE	C.ZIP	X	10	Zip Code Database		2100A/N403	Y	Y	Y			
COUNTY OF RESIDENCE	C.COUNTY	X	2	Data Code Table	161	2100A/N406	Y					
LAST NAME	C.LN	X	32	No CMHC Edit		2100A/NM103	Y	Y	Y	Y		

							Where the Element is used					
Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
FIRST NAME	C.FN	X	25	No CMHC Edit		2100A/NM104	Y	Y	Y	Y		
MIDDLE NAME	C.MN	X	25	No CMHC Edit		2100A/NM105	Y	Y	Y	Y		
CLIENT NAME SUFFIX	C.NMS	X	8	Data Code Table	044	2100A/NM107	Y					
SOCIAL SECURITY NUMBER	C.SSN	X	12	No CMHC Edit		2100A/NM109	Y					
MAILING ADDRESS (1)	C.M.ADD1	X	26	No CMHC Edit		2100C/N301	Y					
MAILING ADDRESS (2)	C.M.ADD2	X	26	No CMHC Edit		2100C/N302	Y					
MAILING CITY	C.M.ADDCIT	X	20	No CMHC Edit		2100C/N401	Y					
MAILING STATE	C.MAILADDS	X	2	Data Code Table	032	2100C/N402	Y					
MAILING ZIP CODE	C.M.ADDZIP	X	10	Zip Code Database		2100C/N403	Y					
MCO ENROLLMENT DATE	$$EN.EFF	D	10	No CMHC Edit		2300/DTP03-356	Y			Y		
PRIMARY MEDICAL INSURANCE	C.INS.PRI	X	1	Data Code Table	154	2320/N102	Y					
SECONDARY MEDICAL INSURANCE	C.INS.SEC	X	1	Data Code Table	154	2320/N102	Y					
TERTIARY MEDICAL INSURANCE	C.INS.TER	X	1	Data Code Table	154	2320/N102	Y					
INTAKE DATE CHANGE	C.INTKCHG	X	1	Data Code Table	105	Y	Y					

HIPAA/837I Health Care Claims/Institutional

Below are the data elements NARBHA uses to prepare the *HIPAA 837 Institutional* data submission transaction as defined in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping is to tie the NARHBA data element/field to the associated element in the *HIPAA 837 Institutional* mapping through the use of the Loop identifier and Abbrev Name (located in the 5th and 9th columns of the *HIPAA 837 Institutional* definition and appearing in the 7th column of the table below). In the *HIPAA 837 Institutional* file definition, many fields are defined as constants, such as "Hierarchical structure Code"/field BHT01/value "0019" or "Entity Identifier Code"/field 1000A-NM101/value "41". These fields, which are required by the 837P, are not mapped to specific NARBHA data elements, but are provided by the CMHC system when generating the transaction. This data transaction has been in production at NARBHA since October 1, 2003, and has been reviewed and approved by ADHS/DBHS staff. Since October 1, 2003, this data submission format has been changed, re-tested, and re-approved.

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
PROVIDER ADDRESS 1	$$PR.ADDR1	X	26	No CMHC Edit		2010AA/N301		Y	Y			
PROVIDER ADDRESS 2	$$PR.ADDR2	X	26	No CMHC Edit		2010AA/N302		Y	Y			
PROVIDER CITY	$$PR.CITY	X	20	No CMHC Edit		2010AA/N401		Y	Y			
PROVIDER STATE	$$PR.STATE	X	2	Data Code Table	032	2010AA/N402		Y	Y			
PROVIDER ZIP	$$PR.ZIP	X	10	No CMHC Edit		2010AA/N403		Y	Y			
CLAIM PROVIDER NAME	CL.PROV.NM	X	12	No CMHC Edit		2010AA/NM103		Y	Y			
ISN STAFF ID	$$ISN.STID	X	6	Staff		2010AA/REF02		Y	Y			
CLAIM FEDERAL TAX ID	CL.FE.TAX	X	9	No CMHC Edit		2010AB/NM109		Y	Y			
BIRTH DATE	C.BD	D	10	Future Date Warning		2010BA/DMG02	Y	Y	Y	Y		
SEX	C.SEX	X	1	Data Code Table	022	2010BA/DMG03	Y	Y	Y			
ADDRESS (1)	C.ADDR1	X	26	No CMHC Edit		2010BA/N301	Y	Y	Y			
ADDRESS (2)	C.ADDR2	X	26	No CMHC Edit		2010BA/N302	Y	Y	Y			
CITY-CLIENT	C.CITY	X	20	No CMHC Edit		2010BA/N401	Y	Y	Y			
STATE	C.STATE	X	2	Data Code Table	032	2010BA/N402	Y	Y	Y			
ZIP CODE	C.ZIP	X	10	Zip Code Database		2010BA/N403	Y	Y	Y			
LAST NAME	C.LN	X	32	No CMHC Edit		2010BA/NM103	Y	Y	Y	Y		
FIRST NAME	C.FN	X	25	No CMHC Edit		2010BA/NM104	Y	Y	Y	Y		
MIDDLE NAME	C.MN	X	25	No CMHC Edit		2010BA/NM105	Y	Y	Y	Y		

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
CIS CLIENT ID	C.AZ.ID	X	10	No CMHC Edit		2010BA/NM109	Y	Y	Y	Y	Y	Y
CLAIM ADMIT HOUR	CL.ADMT.HR	X	4	No CMHC Edit		2300/CL01		Y				
CLAIM PATIENT STATUS	CL.PAT.ST	X	2	No CMHC Edit		2300/CL03		Y				
CLAIM TYPE OF ADMIT	CL.TOA	X	1	No CMHC Edit		2300/CL101		Y				
CLAIM SOURCE OF ADMIT	CL.SOA	X	1	No CMHC Edit		2300/CL102		Y				
ISN ID	$$ISN.ID	X	10	No CMHC Edit		2300/CLM01		Y	Y			
CLAIM PROVIDER INFO 3	$$ISN.CID3	X	32	No CMHC Edit		2300/CLM5-1		Y	Y			
CLAIM ADMIT DATE	CL.ADMT.DT	D	10	No CMHC Edit		2300/DTP03		Y				
CLAIM OCCURRENCE CODE 1	CL.OCCCD1	X	2	No CMHC Edit		2300/HI01-2		Y				
CLAIM PRIMARY DIAGNOSIS	CL.PR.DIAG	X	6	ICD-9 Diagnosis Database		2300/HI01-2		Y	Y			
CLAIM OCCURRENCE DATE 1	CL.OCC.DT1	D	10	No CMHC Edit		2300/HI01-4		Y				
CLAIM ICD 9 CODE 2	C.ICD92	X	6	ICD-9 Diagnosis Database		2300/HI02-2		Y	Y			
CLAIM ICD 9 CODE 4	C.ICD94	X	6	ICD-9 Diagnosis Database		2300/HI04-2		Y	Y			
CLAIM ICD 9 CODE 3	C.ICD93	X	6	ICD-9 Diagnosis Database		2300/HI103-2		Y	Y			
CLAIM DUPLICATE OVERRIDE IND.	CL.DUPOVER	X	1	Data Code Table	029	2300/NTE01		Y	Y			
ISN CREATE DATE	$$ISN.CRDT	D	10	Current Date Warning		2300/NTE02-3		Y	Y			
AUTHORIZATION NUMBER	$$AS.SCNUM	X	20	No CMHC Edit		2300/REF01/G1		Y	Y			
CLAIM AUTHORIZATION NUMBER	$$ISN.CAU	X	20	No CMHC Edit		2300/REF02		Y	Y			
CLAIM ORIGINAL ICN NUMBER	CL.ORIGICN	X	11	No CMHC Edit		2300/REF02/F8		Y	Y			
CLAIM PROVIDER ID	$$ISN.CPID	X	10	Provider Database		2310AA/REF02/1D		Y	Y			

							Where the Element is used					
Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
CLAIM ATTENDING PHYSICIAN ID	CL.ATT.PHY	X	9	No CMHC Edit		2310B/NM109		Y	Y			
CLAIM TPL AMOUNT	CL.TPL.AMT	N	10	No CMHC Edit		2320/AMT01		Y	Y			
MEDICARE ALLOWED AMOUNT	CL.MEDALL	N	9	No CMHC Edit		2320/AMT02/B6		Y	Y			
MEDICARE DEDUCTIBLE	CL.MEDDED	N	9	No CMHC Edit		2320/AMT02/F2		Y	Y			
CLAIM TPL SOURCE CODE	CL.TPL.SRC	X	2	Data Code Table	163	2320/SBR05		Y	Y			
CLAIM TPL CARRIER	CL.TPL.CAR	X	20	No CMHC Edit		2330B/NM103		Y	Y			
CLAIM MODIFIER 1	CL.ST.FMTH	X	2	No CMHC Edit		2400/CL101-3		Y	Y			
MODIFIER 2	CL.ST.TMTH	X	2	No CMHC Edit		2400/CL101-3		Y	Y			
CLAIM CLINICAL PROFILE CLASS	$$ISN.CCPC	X	8	Data Code Table	039	2400/CN101		Y	Y			
CLAIM REMITTANCE AMOUNT PAID	$$ISN.CRPD	N	10	No CMHC Edit		2400/CN102		Y	Y			
CLAIM SERVICE CATEGORY	$$ISN.CSC	X	8	Data Code Table	018	2400/SV101-2		Y	Y			
CLAIM AMOUNT BILLED	$$ISN.CBL	N	10	No CMHC Edit		2400/SV102		Y	Y			
CLAIM UNITS	$$ISN.CUN	N	10	No CMHC Edit		2400/SV104/UN		Y	Y			

HIPAA/837P Health Care Claims/Professional

Below are the data elements NARBHA uses to prepare the *HIPAA 837 Professional* data submission transaction as defined in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping is to tie the NARHBA data element/field to the associated element in the *HIPAA 837 Professional* mapping through the use of the Loop identifier and Abbrev Name (located in the 5th and 9th columns of the HIPAA *837 Professional* definition and appearing in the 7th column of the table below). In the *HIPAA 837 Professional* file definition, many fields are defined as constants, such as “Hierarchical structure Code”/field BHT01/value “0019” or “Entity Identifier Code”/field 1000A-NM101/value “41”. These fields, which are required by the 837P, are not mapped to specific NARBHA data elements, but are provided by the CMHC system when generating the transaction. This data transaction has been in production at NARBHA since October 1, 2003, and has been reviewed and approved by ADHS/DBHS staff. Since October 1, 2003, this data submission format has been changed, re-tested, and re-approved.

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
PROVIDER ADDRESS 1	$$PR.ADDR1	X	26	No CMHC Edit		2010AA/N301		Y	Y			
PROVIDER ADDRESS 2	$$PR.ADDR2	X	26	No CMHC Edit		2010AA/N302		Y	Y			
PROVIDER CITY	$$PR.CITY	X	20	No CMHC Edit		2010AA/N401		Y	Y			
PROVIDER STATE	$$PR.STATE	X	2	Data Code Table	032	2010AA/N402		Y	Y			
PROVIDER ZIP	$$PR.ZIP	X	10	No CMHC Edit		2010AA/N403		Y	Y			
CLAIM PROVIDER NAME	CL.PROV.NM	X	12	No CMHC Edit		2010AA/NM103		Y	Y			
ISN STAFF ID	$$ISN.STID	X	6	Staff		2010AA/REF02		Y	Y			
CLAIM FEDERAL TAX ID	CL.FE.TAX	X	9	No CMHC Edit		2010AB/NM109		Y	Y			
BIRTH DATE	C.BD	D	10	Future Date Warning		2010BA/DMG02	Y	Y	Y	Y		
SEX	C.SEX	X	1	Data Code Table	022	2010BA/DMG03	Y	Y	Y			
ADDRESS (1)	C.ADDR1	X	26	No CMHC Edit		2010BA/N301	Y	Y	Y			
ADDRESS (2)	C.ADDR2	X	26	No CMHC Edit		2010BA/N302	Y	Y	Y			
CITY-CLIENT	C.CITY	X	20	No CMHC Edit		2010BA/N401	Y	Y	Y			
STATE	C.STATE	X	2	Data Code Table	032	2010BA/N402	Y	Y	Y			
ZIP CODE	C.ZIP	X	10	Zip Code Database		2010BA/N403	Y	Y	Y			
LAST NAME	C.LN	X	32	No CMHC Edit		2010BA/NM103	Y	Y	Y	Y		
FIRST NAME	C.FN	X	25	No CMHC Edit		2010BA/NM104	Y	Y	Y	Y		

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
MIDDLE NAME	C.MN	X	25	No CMHC Edit		2010BA/NM105	Y	Y	Y	Y		
CIS CLIENT ID	C.AZ.ID	X	10	No CMHC Edit		2010BA/NM109	Y	Y	Y	Y	Y	Y
ISN ID	$$ISN.ID	X	10	No CMHC Edit		2300/CLM01		Y	Y			
CLAIM PROVIDER INFO 3	$$ISN.CID3	X	32	No CMHC Edit		2300/CLM5-1		Y	Y			
CLAIM PRIMARY DIAGNOSIS	CL.PR.DIAG	X	6	ICD-9 Diagnosis Database		2300/HI01-2		Y	Y			
CLAIM ICD 9 CODE 2	C.ICD92	X	6	ICD-9 Diagnosis Database		2300/HI02-2		Y	Y			
CLAIM ICD 9 CODE 4	C.ICD94	X	6	ICD-9 Diagnosis Database		2300/HI04-2		Y	Y			
CLAIM ICD 9 CODE 3	C.ICD93	X	6	ICD-9 Diagnosis Database		2300/HI103-2		Y	Y			
CLAIM DUPLICATE OVERRIDE IND.	CL.DUPOVER	X	1	Data Code Table	029	2300/NTE01		Y	Y			
ISN CREATE DATE	$$ISN.CRDT	D	10	Current Date Warning		2300/NTE02-3		Y	Y			
AUTHORIZATION NUMBER	$$AS.SCNUM	X	20	No CMHC Edit		2300/REF01/G1		Y	Y			
CLAIM AUTHORIZATION NUMBER	$$ISN.CAU	X	20	No CMHC Edit		2300/REF02		Y	Y			
CLAIM ORIGINAL ICN NUMBER	CL.ORIGICN	X	11	No CMHC Edit		2300/REF02/F8		Y	Y			
CLAIM PROVIDER ID	$$ISN.CPID	X	10	Provider Database		2310AA/REF02/1D		Y	Y			
CLAIM ATTENDING PHYSICIAN ID	CL.ATT.PHY	X	9	No CMHC Edit		2310B/NM109		Y	Y			
CLAIM TPL AMOUNT	CL.TPL.AMT	N	10	No CMHC Edit		2320/AMT01		Y	Y			
MEDICARE ALLOWED AMOUNT	CL.MEDALL	N	9	No CMHC Edit		2320/AMT02/B6		Y	Y			
MEDICARE DEDUCTIBLE	CL.MEDDED	N	9	No CMHC Edit		2320/AMT02/F2		Y	Y			
CLAIM TPL SOURCE CODE	CL.TPL.SRC	X	2	Data Code Table	163	2320/SBR09		Y	Y			

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
CLAIM TPL CARRIER	CL.TPL.CAR	X	20	No CMHC Edit		2330B/NM103		Y	Y			
CLAIM MODIFIER 1	CL.ST.FMTH	X	2	No CMHC Edit		2400/CL101-3		Y	Y			
MODIFIER 2	CL.ST.TMTH	X	2	No CMHC Edit		2400/CL101-3		Y	Y			
CLAIM CLINICAL PROFILE CLASS	$$ISN.CCPC	X	8	Data Code Table	039	2400/CN101		Y	Y			
CLAIM REMITTANCE AMOUNT PAID	$$ISN.CRPD	N	10	No CMHC Edit		2400/CN102		Y	Y			
CLAIM SERVICE CATEGORY	$$ISN.CSC	X	8	Data Code Table	018	2400/SV101-2		Y	Y			
CLAIM AMOUNT BILLED	$$ISN.CBL	N	10	No CMHC Edit		2400/SV102		Y	Y			
CLAIM UNITS	$$ISN.CUN	N	10	No CMHC Edit		2400/SV104/UN		Y	Y			

1

DBHS Demographic

Below are the data elements NARBHA uses to prepare the *CIS Demographic* data submission as defined by the Client Information System (CIS) File Layout Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping is to tie the NARHBA data element/field to the associated element in the *CIS Demographic Data File Format – (T)RBHA Reporting Requirements Field No (column 1)* mapping through the use of the FIELD Identifier (located in the 7th column of the table below). NARBHA mapped the various fields defined in the CIS layout. This data transaction has been in production at NARBHA since July 31, 2003, and has been reviewed and approved by ADHS/DBHS staff. Since August 1, 2003, this data submission format has been changed, re-tested, and re-approved.

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
ASSESSMENT INTERVAL	C.ASSM.INT	X	1	Data Code Table	132	CIS-DEMO-03				Y		
CIS CLIENT ID	C.AZ.ID	X	10	No CMHC Edit		CIS-DEMO-04	Y	Y	Y	Y	Y	Y
MCO ENROLLMENT DATE	$$EN.EFF	D	10	No CMHC Edit		CIS-DEMO-05	Y			Y		
FIRST NAME	C.FN	X	25	No CMHC Edit		CIS-DEMO-06	Y	Y	Y	Y		
MIDDLE NAME	C.MN	X	25	No CMHC Edit		CIS-DEMO-07	Y	Y	Y	Y		
LAST NAME	C.LN	X	32	No CMHC Edit		CIS-DEMO-08	Y	Y	Y	Y		
BIRTH DATE	C.BD	D	10	Future Date Warning		CIS-DEMO-09	Y	Y	Y	Y		
MENTAL HEALTH REFERRAL DATE	C.REF.DATE	D	10	No CMHC Edit		CIS-DEMO-10				Y		
CIF TRANSFER REFERRAL SOURCE	C.TRANS.SR	X	2	Data Code Table	168	CIS-DEMO-11				Y		
OMB-AMERICAN INDIAN	C.OMBAMERI	X	1	Data Code Table	029	CIS-DEMO-12				Y		
OMB-ASIAN	C.OMBASIAN	X	1	Data Code Table	029	CIS-DEMO-13				Y		
OMB-BLACK	C.OMBBLACK	X	1	Data Code Table	029	CIS-DEMO-14				Y		
OMB-NATIVE HAWAIIAN	C.OMBHAWAI	X	1	Data Code Table	029	CIS-DEMO-15				Y		
OMB-WHITE	C.OMBWHITE	X	1	Data Code Table	029	CIS-DEMO-16				Y		
OMB ETHNICITY-HISPANIC-LATINO	C.OMBHISPC	X	1	Data Code Table	029	CIS-DEMO-17				Y		
PRESENTING PROBLEM SUICIDAL	C.PC.SUID	X	1	Data Code Table	029	CIS-DEMO-18				Y		
PRESENTING PROBLEM ASSAULTIVE	C.PC.ASSUA	X	1	Data Code Table	029	CIS-DEMO-19				Y		

							Where the Element is used					
Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
PRESENTING PROBLEM VICTIM ANV	C.PP.VICTI	X	1	Data Code Table	029	CIS-DEMO-20				Y		
PRESENTING PROB ANXIETY/STRESS	C.PP.ANX.S	X	1	Data Code Table	029	CIS-DEMO-21				Y		
PRESENTING PROBLEM DEPRESSED	C.PP.DEPR	X	1	Data Code Table	029	CIS-DEMO-22				Y		
PRESENTING PROBLEM PSYCHOTIC	C.PP.PSYCO	X	1	Data Code Table	029	CIS-DEMO-23				Y		
PRESENTING ISSUES SUBSTANCE AB	C.PI.SUBAB	X	1	Data Code Table	029	CIS-DEMO-24				Y		
PRESENTING ISSUES PERSONAL PRB	C.PI.PER.P	X	1	Data Code Table	029	CIS-DEMO-25				Y		
PRESENTING ISSUE RELATIONSHIP	C.PI.MAR.F	X	1	Data Code Table	029	CIS-DEMO-26				Y		
PRESENTING ISSUES CHILD	C.PI.CHILD	X	1	Data Code Table	029	CIS-DEMO-27				Y		
PRESENTING PROBLEM OTHER	C.PI.OTHER	X	1	Data Code Table	029	CIS-DEMO-28				Y		
PRESENTING PROB BEGIN DATE	C.PC.BDTE	D	10	No CMHC Edit		CIS-DEMO-29				Y		
FAMILY SIZE (INCLUDING CLIENT)	C.FAM.SIZE	X	2	Data Code Table	801	CIS-DEMO-30				Y		
GROSS ANNUAL INCOME	C.FAM.INC	N	10	No CMHC Edit		CIS-DEMO-31				Y		
NATURE OF TREATMENT	C.LEGL.STA	X	1	Data Code Table	164	CIS-DEMO-32				Y		
ST AGENCY ADC	C.ADC	X	1	Data Code Table	029	CIS-DEMO-33				Y		
ST AGENCY ADJC	C.ADJC	X	1	Data Code Table	029	CIS-DEMO-34				Y		
ADHS-CRS	C.ADHS	X	1	Data Code Table	029	CIS-DEMO-35				Y		
ST AGENCY ADULT PROBATION/CRT	C.APCOURT	X	1	Data Code Table	029	CIS-DEMO-36				Y		
ST AGENCY AOC/JPO	C.AOCJPO	X	1	Data Code Table	029	CIS-DEMO-37				Y		
DES-CPS	C.DESCPS	X	1	Data Code Table	029	CIS-DEMO-38				Y		
ST AGENCY DES/DDD	C.DESDD	X	1	Data Code Table	029	CIS-DEMO-39				Y		

							Where the Element is used					
Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
DES-RSA	C.DESRSA	X	1	Data Code Table	029	CIS-DEMO-40				Y		
SCHOOL-SPECIAL ED	C.SCHOOLSE	X	1	Data Code Table	029	CIS-DEMO-42				Y		
ST AGENCY OTHER	C.SAOTHER	X	1	Data Code Table	029	CIS-DEMO-43				Y		
FORMAL SCHOOLING LEVEL	C.FORMSCHL	X	1	Data Code Table	281	CIS-DEMO-45				Y		
OTHER SPECIAL POPULATIONS	C.SPEC.POP	X	3	Data Code Table	144	CIS-DEMO-46				Y		
HB2003 SPECIAL POP	C.HB.SPOP	X	2	Data Code Table	616	CIS-DEMO-47				Y		
PREGNANT WOMAN/DEP. CHILD(REN)	C.AZ.PRGNT	X	1	Data Code Table	029	CIS-DEMO-49				Y		
WOMAN WITH DEPENDENT CHILD	C.AZ.WDC	X	1	Data Code Table	029	CIS-DEMO-50				Y		
DIAGNOSIS CODE AXIS III	C.DX.III	X	2	Data Code Table	049	CIS-DEMO-52				Y		
DSM-IV AXIS III SECONDARY	C.AXISIII2	X	2	Data Code Table	049	CIS-DEMO-53				Y		
DSM-IV AXIS III TERTIARY	C.AXISIII3	X	2	Data Code Table	049	CIS-DEMO-54				Y		
DIAGNOSIS CODE AXIS III-4	C.DX.III4	X	2	Data Code Table	049	CIS-DEMO-55				Y		
DIAGNOSIS CODE III-5	C.DX.III5	X	2	Data Code Table	049	CIS-DEMO-56				Y		
DATE DIAGNOSIS ASSESSED	C.DX.DATE	D	10	Window Date Warning		CIS-DEMO-57				Y		
ICD-9 BILLING DIAGNOSIS	C.BILLDIAG	X	10	ICD-9 Diagnosis Database		CIS-DEMO-58				Y		
ICD-9 BILLING DIAGNOSIS-SECOND	C.ICD9.2ND	X	10	DSM-IV Axis I Diagnosis D		CIS-DEMO-59				Y		
ICD-9 BILLING DIAGNOSIS-THIRD	C.ICD9.3RD	X	10	DSM-IV Axis I Diagnosis D		CIS-DEMO-60				Y		
ICD-9 BILLING DIAGNOSIS-FOURTH	C.ICD9.4TH	X	10	DSM-IV Axis I Diagnosis D		CIS-DEMO-61				Y		
DIAGNOSIS CODE AXIS I-5	C.DX.I.5	X	8	ICD-9 Diagnosis Database		CIS-DEMO-62				Y		
DIAGNOSIS CODE AXIS II PRIMARY	C.DX.IIPRI	X	6	ICD-9 Diagnosis Database		CIS-DEMO-63				Y		

Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	Where the Element is used					
							834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
DIAGNOSIS CODE AXIS II SECOND	C.DX.IISEC	X	6	ICD-9 Diagnosis Database		CIS-DEMO-64				Y		
POPULATION	C.POP	X	1	Data Code Table	153	CIS-DEMO-65				Y		
ASMT REHABILITATION STATUS	C.ASMT.REH	X	2	Data Code Table	125	CIS-DEMO-66				Y		
EDUCATIONAL STATUS	C.EDUCSTAT	X	1	Data Code Table	029	CIS-DEMO-67				Y		
RESID. ARRANGEMENT	C.RES.ARAG	X	2	Data Code Table	122	CIS-DEMO-69				Y		
DIAGNOSIS CODE AXIS V	C.DX.V	X	8	Data Code Table	052	CIS-DEMO-70				Y		
NUM OF ARRESTS DURING PAST YR	C.#.ARREST	X	2	No CMHC Edit		CIS-DEMO-71				Y		
PRIMARY DRUG PROBLEM	C.DRG.PRI	X	8	Data Code Table	121	CIS-DEMO-72				Y		
PRIMARY DRUG FREQUENCY OF USE	C.DRG.PFOU	X	8	Data Code Table	081	CIS-DEMO-73				Y		
PRIMARY DRUG ROUTE OF ADMIN	C.DRG.PROA	X	8	Data Code Table	082	CIS-DEMO-74				Y		
PRIMARY DRUG AGE OF 1ST USE	C.DRG.PAFU	X	2	No CMHC Edit		CIS-DEMO-75				Y		
SECONDARY DRUG PROBLEM	C.DRG.SEC	X	8	Data Code Table	121	CIS-DEMO-76				Y		
SECONDARY DRUG FREQ OF USE	C.DRG.SFOU	X	8	Data Code Table	081	CIS-DEMO-77				Y		
SECONDARY DRUG ROUTE OF ADMIN	C.DRG.SROA	X	8	Data Code Table	082	CIS-DEMO-78				Y		
SECONDARY DRUG AGE OF 1ST USE	C.DRG.SAFU	X	2	No CMHC Edit		CIS-DEMO-79				Y		
DRUG ADDITIONAL DRUG	X.ADATYPE	X	4	Data Code Table	121	CIS-DEMO-80				Y		
REASON FOR DISCHARGE	C.AZ.DSCH2	X	2	Data Code Table	434	CIS-DEMO-81				Y		

1

Retail Pharmacy Claims Processing (Request)

Below are the data elements NARBHA uses to prepare the *NCPDP–Retail Pharmacy Claims Processing (Request)* data submission transaction as defined in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping is to tie the NARHBA data element/field to the associated element in the *NCPDP–Retail Pharmacy Claims Processing (Request)* mapping through the use of the FIELD Identifier (located in the 7th column of the table below). In the *NCPD–Retail Pharmacy Claims Processing (Request)* file definition, many fields are either defined as constants ("Version/Release number"/field 102-A2/value "51") or marked as N/A under the input field ("Segment Identifier"/field 111-AM/value "04"). These fields, which are required by the NCPDP, are not mapped to specific NARBHA data elements, but are provided by the CMHC system when generating the transaction. This data transaction has been in production at NARBHA since October 1, 2003, and has been reviewed and approved by ADHS/DBHS staff. Since October 1, 2003, this data submission format has been changed, re-tested, and re-approved.

							Where the Element is used					
Data Element Name	**Short Name**	**Data Type**	**Len**	**Data Field Validation**	**Data Field Validation Table**	**Map Ref**	**834/Enroll**	**837/Inst**	**837/Prof**	**Demographics**	**NCPDP**	**NCPDP/Supp.**
GENERATED ICN NUMBER	ER02KEY	N	10			104/A4					Y	
NABPID	NCPDP	X	9	valid NCPDP ID		201/B1					Y	
RBHA ID	RBHAID	X	2	value "15"		301/C1					Y	
CIS CLIENT ID	C.AZ.ID	X	10	No CMHC Edit		302/C2	Y	Y	Y	Y	Y	Y
CARDHLDRID	CLIENTID	X	10	Valid member		302/C2					Y	
DATE FILLED	DTFILLED	D	8	valid date		401/D1					Y	
PRESCRIPTION NUMBER	RX	X	7	N/A		402/D2					Y	
REFILL INDICATOR	NEWREFILL	N	2	N/A		403/D3					Y	
PAID DAYS SUPPLY	PPDAYSSUPLY	N	3	> 0		405-D5					Y	
NDCCODE	NDCCODE	X	11	Valid NDC code		407/D7					Y	
INGREDIENT COST	INDCOSTPD	N	8	> 0		409/D9					Y	
PRESCRIBER ID	DOCTORNUM	X	15	Valid DEA Number		411/DB					Y	
DISPENSING FEE	DISPFEE	N	8	> or = 0		412/DC					Y	
DATA SCRIPT WRITTEN	DATEWRIT	D	8	valid date		414/DE					Y	
REFILL ALLOWED	REFILLAUTH	X	2	N/A		415/DF					Y	
QUANTITY	QUANTITY	N	4	> 0		422/E7					Y	
BILLER AMOUNT	BILLEDAMT	N	8	> or = 0		430/DU					Y	
PATIENT PAID AMOUNT	MBRRESP	N	8	> or = 0		433/DX					Y	

Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	Where the Element is used					
							834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
PROCEDURE CODE MODIFIER	MODIFIER	X	2	always blank		459/ER					Y	

NCPDP Supplemental

Below are the data elements NARBHA uses to prepare the *Encounter Drug Supplemental File Layout* data submission transaction as defined in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004). The methodology for this mapping has been to tie the NARHBA data element/field to the associated element in the Encounter Drug Supplemental File Layout mapping through the use of the RECORD LOCATION FROM/TO fields documented in the first and second columns of that file layout. An example is the RBHA-ID, which is in RECORD LOCATION FROM "2"/TO "3." NARBHA's map reference for its internal RBHA ID is labeled below as "EDS/2-3." This data transaction is new and is currently being tested between this RBHA and ADHS/DBHS. Depending on direction from ADHS/DBHS and the Arizona Health Care Cost Containment Systems (AHCCCS) staff, it may be amended.

Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref	Where the Element is used					
							834/Enroll	837/Inst	837/Prof	Demographics	NCPDP	NCPDP/Supp.
CIS ID	C.AZ.ID	X	10	valid CIS ID		EDS/4-13	Y	Y	Y	Y	Y	Y
GENERATED ICN NUMBER	ER02KEY	N	10	Internal NARBHA control number		EDS/14-23						Y
RBHA ID	RBHAID	X	2	value "15"		EDS/2-3						Y
OTHER INSURANCE DISPENSING FEE	OINSDISPF	N	8	> or = 0		EDS/24-31						Y
OTHER INSURANCE INGREDIENT COST	OINSINDCST	N	8	> or = 0		EDS/32-39						Y
OTHER INSURANCE CO-PAY AMT	OINSCOPAY	N	8	> or = 0		EDS/40-47						Y
OTHER INSURANCE DEDUCTIBLE AMT	OINSDEDU	N	8	> or = 0		EDS/48-55						Y
OTHER INSURANCE COINSURANCE AMT	OINSCOINS	N	8	> or = 0		EDS/56-63						Y
MEDICARE DISPENSING FEE	MCARDISPF	N	8	> or = 0		EDS/64-71						Y
MEDICARE INGREDIENT COST	MCARINDCST	N	8	> or = 0		EDS/72-79						Y
MEDICARE CO-PAY AMT	MCARCOPAY	N	8	> or = 0		EDS/80-87						Y
MEDICARE DEDUCTIBLE AMT	MCARDEDU	N	8	> or = 0		EDS/88-95						Y
MEDICARE COINSURANCE AMT	MCARCOINS	N	8	> or = 0		EDS/96-113						Y

DATA ELEMENTS LISTED THAT ARE NOT CURRENTLY CAPTURED, STORED, OR USED

Based on the specifications and requirements set forth in the Client Information System (CIS) File Layout and Specification Manual (ver1.19 revision date 8/02/2004), NARBHA is able to satisfy all requirements for data capture and submission at this time with the following single exception.

NCPDP Supplemental

The proposed requirement for data capture and submission pertaining to third party reimbursement, including insurance and Medicare, are still in the design phase. NARHBA is diligently working with its current Pharmacy Benefits Management (PBM) firm, CaremarkPCS, to determine the operational considerations in capturing this information. The challenges center on the availability of information any PBM might consider proprietary and may choose not to disclose. The ability to submit information in the accepted format, from a technical perspective, is well within the ability of NARBHA MIS staff to perform. The ability to capture this data is still in the design phase.

Data Element Name	Short Name	Data Type	Len	Data Field Validation	Data Field Validation Table	Map Ref
OTHER INSURANCE DISPENSING FEE	OINSDISPF	N	8	> or = 0		EDS/24-31
OTHER INSURANCE INGREDIENT COST	OINSINDCST	N	8	> or = 0		EDS/32-39
OTHER INSURANCE CO-PAY AMT	OINSCOPAY	N	8	> or = 0		EDS/40-47
OTHER INSURANCE DEDUCTIBLE AMT	OINSDEDU	N	8	> or = 0		EDS/48-55
OTHER INSURANCE COINSURANCE AMT	OINSCOINS	N	8	> or = 0		EDS/56-63
MEDICARE DISPENSING FEE	MCARDISPF	N	8	> or = 0		EDS/64-71
MEDICARE INGREDIENT COST	MCARINDCST	N	8	> or = 0		EDS/72-79
MEDICARE CO-PAY AMT	MCARCOPAY	N	8	> or = 0		EDS/80-87
MEDICARE DEDUCTIBLE AMT	MCARDEDU	N	8	> or = 0		EDS/88-95
MEDICARE COINSURANCE AMT	MCARCOINS	N	8	> or = 0		EDS/96-113

NARHBA has been working with files provided by ADHS/DBHS since 1994, when files were first passed to ADHS/DBHS from EDS Data Systems and on to the various Regional Behavioral Health Authorities (RBHAs). Since that time, NARBHA has gained a vast amount of expertise in the uses of these various files, the technologies for exchanging these files, and the manners in which the files interrelate. The wealth of NARBHA-specific information submitted to ADHS/DBHS (enrollment, demographic, claims, medications), when linked to data in files from ADHS/DBHS (State Roster, At Risk, Third Part Liability, etc.) and then combined with information specific to projects at NARHBA (CPS 24-hour Response, Institutions for Mental Disease (IMD), Substance Abuse and Treatment (SAPT), etc.) provides a complete picture of the NARBHA environment and allows accurate and efficient monitoring of service delivery in the NARBHA geographic service area.

There are multiple data flows between NARBHA and ADHS/DBHS as well as among NARBHA and its Service Area Agencies (SAAs), Tribal Area Agencies (TAAs), and fee-for-service (FFS) and single case agreement (SCA) providers; each of these data flows is diagrammed and described in detail below. The ways in which the NARBHA system defines edit criteria and applies these edits to all input data, regardless of how such data enters the system, also are explained in this section.

Use of State Roster Files

The State Roster Files contain data about all members currently or previously enrolled at all RBHAs. Three components of data are involved:

- data about members
- data about all enrollment segments
- data about member eligibility segments

NARBHA's Management Information Systems Department (MIS) pulls the State Roster data daily for incremental updates, and pulls the full refresh files each Monday. From the basic State Roster data file, NARBHA MIS prepares three separate daily files for NARBHA's use:

- Member file
- Enrollment file
- Eligibility file

MIS extracts key fields from these three files, compresses the files, and places them on NARBHA's File Transfer Protocol (FTP) server. Each of NARBHA's SAAs retrieves the files to use in local applications. This provides current data on a daily basis for NARBHA's SAAs. In addition, NARBHA's Member Service Representatives use the State Roster data to assist in resolving inter-RBHA issues.

These data are used for several key programs at NARBHA and at NARBHA's SAAs. NARBHA MIS developed an inquiry software package known as Intelligent Global Gathering Information (IGGI), which is available to all SAAs at no cost. The data to support IGGI come from the NARBHA CMHC-MCO system (a component of NARBHA's main production system, detailed in Volume 5.b), and the State Roster data files. IGGI allows staff at NARBHA and its SAAs to verify personal data and current enrollment status for all new and returning members. All eligible Title XIX and Title XXI segments are displayed in IGGI to help the SAAs better serve their members.

Several of NARBHA's custom-developed applications such as CASPER834 and CASPERCompanion (detailed in Volume 5.b) use the State Roster data to ensure that correct edits are applied when receiving data from NARBHA's SAAs/TAAs. Please refer to the 834 Flow of Data section below for specifics as to how these data are used in these applications.

Use of Intelligent Global Gathering of Information (IGGI)

The IGGI application contains information about all members in the NARBHA CMHC-MCO system as well as members who have been enrolled at other RBHAs throughout Arizona. IGGI has several main functions, the most important being the data lookup screen. This screen displays member demographics, enrollment segments, and all eligibility segments, both in NARBHA's CMHC-MCO system and the State Roster files. IGGI allows users to easily research data from both sources, and it makes comparisons to highlight data discrepancies between the two data sources, such as different Social Security Numbers (SSNs). In addition, IGGI offers several methods to locate the correct member: Member ID (commonly known as the BHMIS ID), the ADHS/DBHS-generated unique member ID (known as the CIS ID), Arizona Health Care Cost Containment System (AHCCCS) ID, SSN, or member name.

IGGI also offers some key reporting functions. NARHBA MIS has developed reports to balance internal admits and closures with ADHS/DBHS admits and closures for NARBHA, allowing NARBHA MIS to review and resubmit any data necessary. NARBHA MIS also has developed IGGI-based reports to indicate to the SAAs when particular member data are due for submission to NARBHA.

Member ID Cross Reference

NARBHA and its SAAs/TAAs assign a member ID in the old style, which consists of member's first initial, member's last initial, member's date of birth, member's gender, and a "tie breaker" commonly referred to as a BMHIS ID. NARBHA and the SAAs/TAAs made this decision in 1997 when ADHS/DBHS changed to the numeric ID assignment. The decision has been well received because the SAAs/TAAs find it critical to correctly assign an ID at admit time.

NARBHA MIS keeps a one-to-one cross-reference database table and updates it daily during the download Intake processing. If a CIS ID is received that is not currently in the cross-reference table, a new record is added that has data for the CIS ID and the NARBHA SAA/TAA member ID, as well as the date added. If the CIS ID received is already in the cross-reference table, incoming data are compared to data in the table for correctness. If a discrepancy exists, a message and report are generated and reviewed. Upon completion of the Intake download process, any new CIS IDs are extracted, formatted, and imported into the NARBHA CMHC-MCO system to be used for claims submission, 834 Discharges, demographic submission, and any other process requiring the CIS ID.

NARBHA MIS has developed a lookup system that allows NARBHA and SAA staff to search for members using either or both the NARBHA SAA/TAA ID and the CIS ID.

DATA SUBMISSION

Data submission is defined as the submission of electronic information to ADHS/DBHS from NARBHA, with electronic feedback to NARBHA on how that information was processed, accepted, and returned to NARBHA. The processes below address the submission and return of information for:

- Intake and Closure (HIPAA 834)
- Institutional Claims (HIPAA 837/1)
- Professional Claims (HIPAA 837/)
- Pharmacy Claims Retail (HIPAA HCPDP)
- Pharmacy Claims Retail Supplemental (ADHS/DBHS-defined)
- ADHS/DBHS Demographic

834 Flow of Data

ADHS/DBHS requires NARBHA to receive and submit data for the Health Insurance Portability and Accountability Act (HIPAA)-compliant ASC X12N 834 Benefit Enrollment and Maintenance Transaction Format. Using the HIPAA mapping documents provided by ADHS/DBHS, NARBHA receives data daily from its SAAs/TAAs. After a thorough editing process designed to mirror ADHS/DBHS edits, data are accepted into NARBHA's CMHC-MCO system, and then turned around the same day to submit HIPAA-compliant 834 transactions to ADHS/DBHS. This assures data are submitted timely and accurately.

As Diagram 5.k.1 illustrates, 834 Admit Data (enrollments) and 834 Discharge Data (disenrollments) are received at NARBHA from the SAAs/TAAs. Data are received from the SAAs completely electronically, entered remotely at the SAA site and transferred daily to NARBHA. Data received from the TAAs are faxed daily to NARBHA for entry into discrete CMHC systems that support each TAA. From this point forward, all data submitted electronically from an SAA or faxed and entered into a discrete system for a TAA are handled identically, using the same programs, processes, and defined edits.

Data Flow at the SAAs/TAAs

SAAs/TAAs submitting data electronically to NARBHA enter data locally into the common data system, CMHC-MCO. This is a flexible data system that is easily modified to allow NARBHA, as well as the SAAs/TAAs, to stay current on all data needs. The system is set up to require data entry for all national, state, and local requirements, and the entry tables are defined to allow only valid data to be entered. After data are submitted, and validated, they are extracted from the data system and run through a local copy of the data validation program Collection and Scanning Program Edit Reporting (CASPER834), developed by NARBHA MIS. CASPER834 edits both 834 Admit Data and 834 Discharge Data for proper field content, accuracy of data, and reasonableness of data, and verifies data fields for correct length and correct values. Data fields are scanned for non-allowable characters such as non-numeric values in a member SSN. CASPER834 uses the entire data set extracted to cross-verify data, such as requiring a city in Northern Arizona if the county/Federal Information Processing Standards (FIPS) code indicates a Northern Arizona address. CASPER834 also uses data provided by ADHS/DBHS, known as the State Roster, to verify the Admit/Discharge data will not overlap with other Admits/Discharges for another RBHA in the state. The State Roster data are also used to validate specific identifying information such as member AHCCCS ID, member SSN, member gender, and member date of birth. If additional research is needed to correct any data indicated in error, the SAA/TAA staff reviews and updates the data set.

When all possible edits are applied and reviewed for accuracy, the SAA/TAA staff creates a sequential HIPAA 834 Admit file and a sequential HIPAA 834 Discharge file adhering to exact national standards. These files are transferred to NARBHA via a secure FTP process.

Data Flow at NARBHA

NARBHA processes all files transferred to the FTP server each afternoon, Monday through Friday, using a CMHC translator/reader. The translator is parameter-driven to allow flexibility in defining data elements to translate. The data are read into a special database file specific to inbound 834 processing. The same data are then extracted for edit purposes at NARBHA and the same edits (CASPER834) are run, with one additional edit based on duplicate submission of data on the same member either by multiple SAAs/TAAs or the same SAA/TAA.

Upon successful completion of CASPER834 in MCO mode, reports are generated and data import files are created to write the 834 Admits and 834 Discharges into NARBHA's permanent CMHC-MCO system. These same Admits and Discharges are combined with any Admits and Discharges previously received that need modification. An additional process is run to verify that all required data are present and valid. This is done mainly to re-edit older admits that may need to be resubmitted to AHDH/DBHS. If any data are missing or incomplete, the Admit and/or Discharge is not included in the sequential file creation. This ensures that the data sent to ADHS/DBHS do not fail the ADHS/DBHS translator, invalidating the entire file.

Data Flow to ADHS/DBHS

NARBHA MIS then creates sequential 834 Admit and Discharge files to submit to ADHS/DBHS and transfers the files to the ADHS/DBHS FTP server, known as Sherman, through a secure FTP process.

Data Flow back to NARBHA

The next morning NARBHA MIS retrieves all data files available from ADHS/DBHS to include download data files, download error files, and download control files. The control file is retrieved to check which data files have been created. Using the counts on the control file, NARBHA MIS staff retrieves additional data files and applies them to NARBHA's internal database tables, which are used for reporting, analysis, and data reconciliation. NARBHA MIS also retrieves any error files to create reports for any necessary research. These reports are separated by demographic data and assigned to specific staff within MIS. MIS staff research these reports daily and, if unable to resolve a case, send it to the MIS production manager for resolution. This allows MIS to perform daily submissions to ADHS/DBHS in a timely manner as well as eliminating possible problems with inter-RBHA enrollments.

NARBHA also retrieves data common to all RBHAs, including the State Roster and Third Party Liability (TPL) file. The State Roster file is parsed and split into three categories:

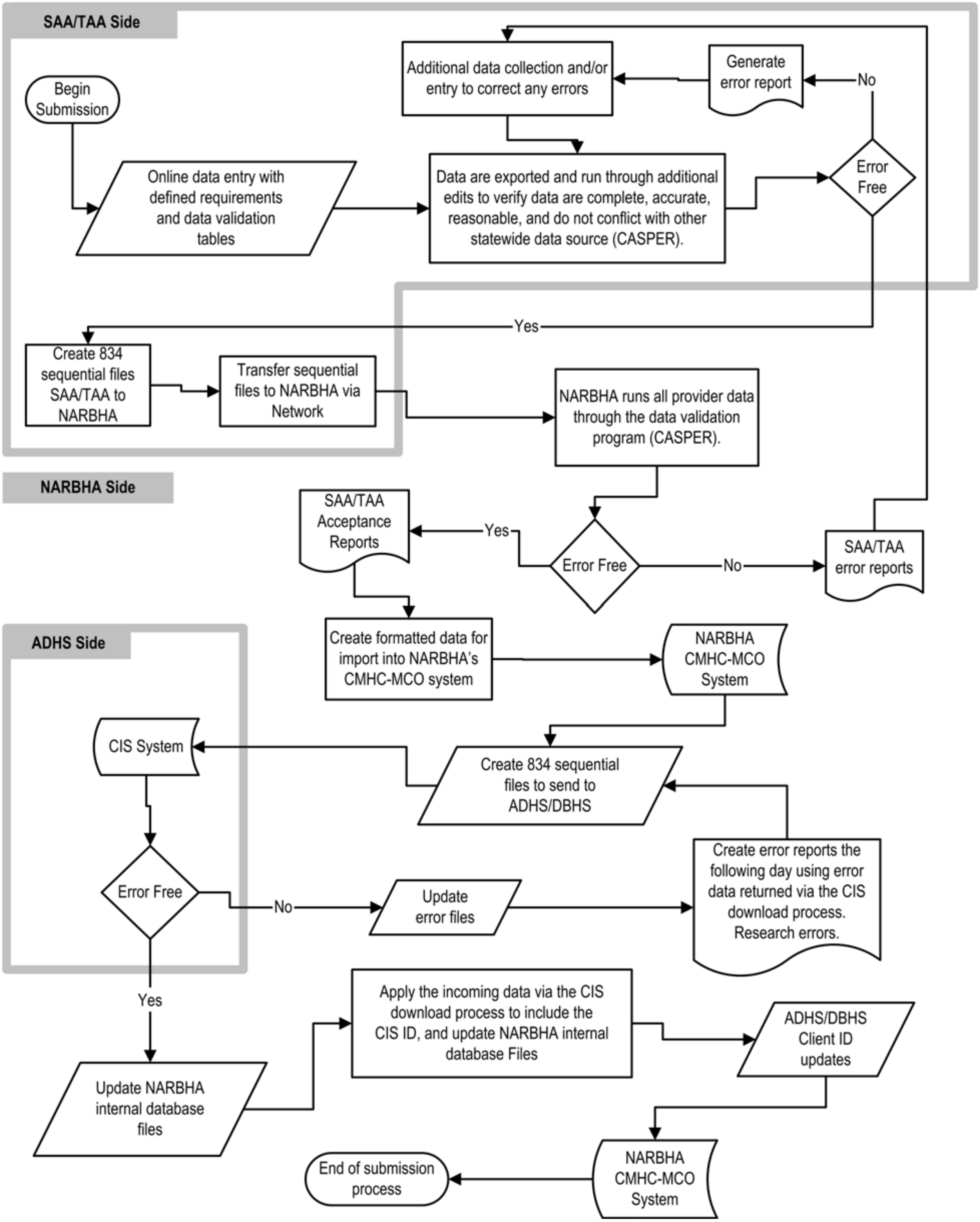
- Members
- Enrollments
- Eligibility

These data are then applied to a database table and used in several processes including a lookup system to allow necessary staff access to information and the above edit application, CASPER834, to verify all incoming data.

Several key data elements are returned through the download process. The CIS ID is returned with the downloaded Intakes, and NARBHA's internal cross-reference file refers back to NARBHA's assigned member ID. These IDs are then updated into NARBHA's CMHC-MCO system. Additionally, if ADHS/DBHS returns an AHCCCS ID that is "not defined" or "does not match NARBHA's CMHC-MCO AHCCCS ID," an AHCCCS ID report and import file is generated. The report is reviewed for accurate data both at NARBHA and distributed to the appropriate SAA/TAA. The AHCCCS ID is then imported into NARBHA's CMHC-MCO.

NARBHA's 834 admit and discharge data flow is shown in Diagram 5.k.1.

Diagram 5.k.1 834 Admit and Discharge Data Flow


SAA/TAA Side
Begin Submission
Online data entry with defined requirements and data validation tables
Data are exported and run through additional edits to verify data are complete, accurate, reasonable, and do not conflict with other statewide data source (CASPER).
Error Free
No
Generate error report
Additional data collection and/or entry to correct any errors
Yes
Create 834 sequential files SAA/TAA to NARBHA
Transfer sequential files to NARBHA via Network
NARBHA Side
NARBHA runs all provider data through the data validation program (CASPER).
Error Free
Yes
SAA/TAA Acceptance Reports
No
SAA/TAA error reports
Create formatted data for import into NARBHA's CMHC-MCO system
NARBHA CMHC-MCO System
ADHS Side
CIS System
Create 834 sequential files to send to ADHS/DBHS
Error Free
No
Update error files
Create error reports the following day using error data returned via the CIS download process. Research errors.
Yes
Update NARBHA internal database files
Apply the incoming data via the CIS download process to include the CIS ID, and update NARBHA internal database Files
ADHS/DBHS Client ID updates
NARBHA CMHC-MCO System
End of submission process

1

Demographic/Companion Flow of Data

ADHS/DBHS requires that NARBHA submit Client Information System (CIS) Demographic data as defined by the CIS File Layout Specification Manual (ver1.19 revision date 8/02/2004). ADHS/DBHS then uses these data in conjunction with other information in the CIS system to prepare reports and analyses. NARBHA gathers this CIS Demographic information from its SAAs and TAAs through what it defines as a "Companion" data set. This Companion data set contains all the elements defined in the CIS Demographic file specification as well as additional information NARBHA uses to manage its business. The edits applied to the data in this Companion data set are the same edits that ADHS/DBHS applies to the CIS Demographic file when NARBHA submits it to ADHS/DBHS, plus NARBHA internal edits applied to its specific data.

NARBHA receives daily Companion data sets from its SAAs/TAAs. After a thorough editing process designed to mirror ADHS/DBHS edits applied to the Demographic data, the Companion data sets are accepted into NARBHA's CMHC-MCO system. That information is submitted to ADHS/DBHS as Demographic data later that same day.

As Diagram 5.k.2 illustrates, NARBHA's Companion data sets are received from its SAAs/TAAs daily. Data are received from NARBHA's SAAs completely electronically. Data received from NARBHA's TAAs are faxed daily to NARBHA for entry locally into a system dedicated to each TAA. From this point forward, all data submitted electronically from an SAA or faxed and entered into a discrete system for a TAA are handled identically, using the same programs, processes, and defined edits.

<u>Data Flow at the SAAs/TAAs</u>

SAAs/TAAs submitting data electronically to NARBHA enter data locally into the common data system, CMHC-MCO. The system is set up to require data entry that adheres to all state and local requirements. Data entry tables are defined to allow only valid data to be entered. Data are then extracted from the SAA's/TAA's data system and run through a local copy of the data validation program CASPERCompanion, developed by MIS. CASPERCompanion edits any data required by NARBHA but not defined on the 834 Admit or 834 Discharge Data definition (NARBHA's Companion data). These data are edited for proper field content, accuracy, and reasonableness. Data fields are verified for correct length and correct values. CASPERCompanion uses the entire data set extracted to cross-verify data such as certain special populations not valid for male members. If additional research is needed to correct any data indicated in error, the SAA/TAA staff reviews and updates the data set.

When all possible edits are applied and reviewed for accuracy, the SAA/TAA staff transfers the exported data to NARBHA via a secure FTP process.

<u>Data Flow at NARBHA</u>

NARBHA processes all Companion data transferred to its secure FTP server each afternoon after processing the 834 data. This allows providers to submit both the 834 data and the accompanying Companion data the same day. While this is not a requirement, most providers prefer to submit both data sets together. The same edits (CASPERCompanion) are run at NARBHA as were run at the SAAs/TAAs, using data submitted from all SAAs/TAAs.

Upon successful completion of CASPERCompanion edits at NARBHA, reports are generated and data import files are created to write the Companion data into NARBHA's permanent CMHC-MCO system.

<u>Data Flow to ADHS/DBHS</u>

NARBHA's Companion data are used to create demographic data. MIS then creates the defined ADHS/DBHS demographic file and transfers it daily to the ADHS/DBHS FTP server, known as Sherman, via secure FTP.

<u>Data Flow back to NARBHA</u>

The next morning NARBHA MIS retrieves both the download Demographic file and any errors that may have been found by ADHS/DBHS. MIS applies the data file to NARBHA's Demographic database table, formats the errors into an easy reporting system, separates the reports by Demographic data, and assigns the reports to specific MIS staff. Reports are researched daily and, if a staff member is unable to resolve a case, the case is sent to the MIS production manager. This allows NARBHA MIS to perform daily submissions in a timely manner.

If a CIS ID has not yet been assigned to a member, the Demographic is marked “pending” and automatically resubmitted the next working day. This minimizes the time to submit demographic data.
NARBHA has defined three major Companion types, including two types of Admit companions:

- Admit Companion data are due for all members within 14 days of the Admit date. This contains data not defined on an Admit 834 but essential for NARBHA. Such data elements include the member’s general health category, diagnosis data, referral date, and other data that allow NARBHA to measure key indicators and to submit data to ADHS/DBHS in the Demographic format. For all members who remain enrolled for 45 or more days, a full Admit Companion is required, which completes the submission of the ADHS/DBHS Demographic data.

- Annually, or when significant changes occur for the member, a full During Treatment Companion is submitted.

- Upon discharge, a Discharge Companion is required. The requirements vary based on the length of the enrollment segment. A complete Discharge Companion, as defined by ADHS/DBHS, is required for all members who remain in the system for 45 days or longer. For short-term enrollments, NARBHA has defined a slightly less complete data set that satisfies ADHS/DBHS and NARBHA requirements.

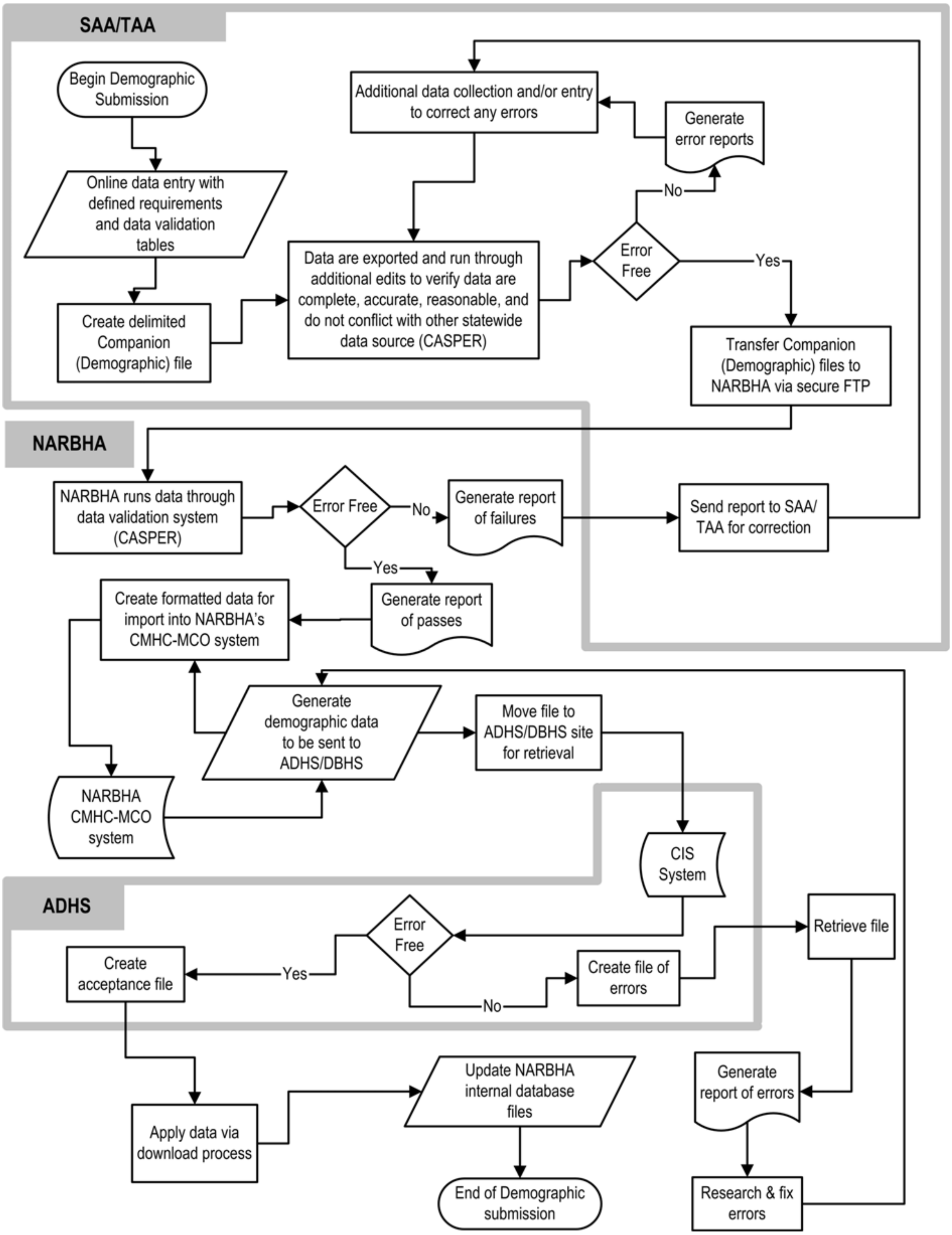
NARBHA MIS requires that Companion data be received in the correct order. A “last Companion type” is stored in NARBHA’s CMHC-MCO system and compared to incoming data. Additionally, NARBHA MIS has developed reports that can be run locally by all SAAs/TAAs to track Companion needs. These include all Companion types.

NARBHA MIS recently created two additional processes to ensure timely Demographic submission. The first is the ability to compare Enrollments to initial Demographics and identify missing Demographics. The second process is to rebuild any missing Demographics and re-submit.

NARBHA’s demographic data flow is shown in Diagram 5.k.2.

Diagram 5.k.2

Demographic Data Flow


SAA/TAA
Begin Demographic Submission
Online data entry with defined requirements and data validation tables
Create delimited Companion (Demographic) file
Data are exported and run through additional edits to verify data are complete, accurate, reasonable, and do not conflict with other statewide data source (CASPER)
Error Free
No
Generate error reports
Additional data collection and/or entry to correct any errors
Yes
Transfer Companion (Demographic) files to NARBHA via secure FTP
NARBHA
NARBHA runs data through data validation system (CASPER)
Error Free
No
Generate report of failures
Send report to SAA/ TAA for correction
Yes
Generate report of passes
Create formatted data for import into NARBHA's CMHC-MCO system
NARBHA CMHC-MCO system
Generate demographic data to be sent to ADHS/DBHS
Move file to ADHS/DBHS site for retrieval
CIS System
ADHS
Error Free
Yes
Create acceptance file
No
Create file of errors
Retrieve file
Generate report of errors
Research & fix errors
Apply data via download process
Update NARBHA internal database files
End of Demographic submission

1

Claims/Encounters Processing Flow of Data

Claims defined as "type of service one" are claims where the provider receives a check payment for services rendered. Encounters defined as "type of service two" are claims where the provider receives a credit toward services rendered. Both of these claims/encounters will be referred to as claims in this document.

The Claims processing system at NARBHA is designed to receive data from all providers (SAAs/TAAs/FFSs/SCAs). These claim data files are validated based upon many claiming rules. Once the data files are validated they are submitted to ADHS/DBHS.

Data Flow at the SAAs/TAAs/FFSs/SCAs

All providers can submit data to NARBHA in three ways:

- Data files are received from providers in HIPAA 837 Professional or HIPAA 837 Institutional formats, which are transferred through a secure T1 line and placed in a single provider's directory on the NARBHA CMHC/UNIX host.
- Data are received from providers on paper using a 1500 HCFA or UB92 Claim form, which is then entered into the CMHC-CLM system and stored in a holding database.
- Providers may choose to enter data directly into NARBHA's CMHC-CLM holding database.

Data Flow at NARBHA

Claim files are *copied* from the provider's directories to a NARBHA archive directory for each individual provider, where a "snapshot" of the file names is taken before processing. This snapshot report is sent to each of the providers via FTP, showing that the files are being processed with a system date stamp. The files are then copied to an overall processing directory and removed from the directory where the providers submitted the files.

Once the claims are copied they are then *prepared*. This process runs the claims through edits to check for valid provider data and valid HIPAA 837 formats. If the claims pass the *prepared* step, the file moves on; if they fail the *prepared* step, the file is not processed, and the provider is notified by e-mail that the files failed and they need to be corrected and resubmitted.

Claims are then *merged* and *processed*. This process takes all claim files and processes the first set of edits against the files. These edits include:

- Service date and enrollment edits
- Duplicate edits
- Service authorization edits
- Contract edits

All claims are then *exported* into a holding database for additional validation. Claim validation includes, but is not limited to:

- Medicare edits
- Admit/discharge/bill type edits
- Claim over six months old
- Provider type edits
- Ancillary claim edits
- Diagnosis code edits

All claims are run through approximately 60 additional validation rules to ensure the accuracy of the data. All edit data are then written to the holding database as approved or denied claims and passed on to the posting process to be added to the CMHC-MCO claims database.

Uscript is a scripting language within CMHC to allow reading and writing of data. NARBHA uses Uscript to perform edits on modifier, place of service, and service code edit; this process approves or denies the claims based on the edit rules. Uscript also processes data to compare remittance amounts paid against billed amounts for reporting purposes. Stratification reports are run after all edits are complete and errors are corrected.

All claims are *posted* to the production database (DB09). From DB09, data are exported to generate Explanation of Benefits (EOBs) and HIPAA 835 Electronic EOB files. These files are placed in each provider's directory through a secure FTP connection for download to the providers. EOBs also are printed and sent to providers that do not have FTP capabilities.

Data Flow to ADHS/DBHS

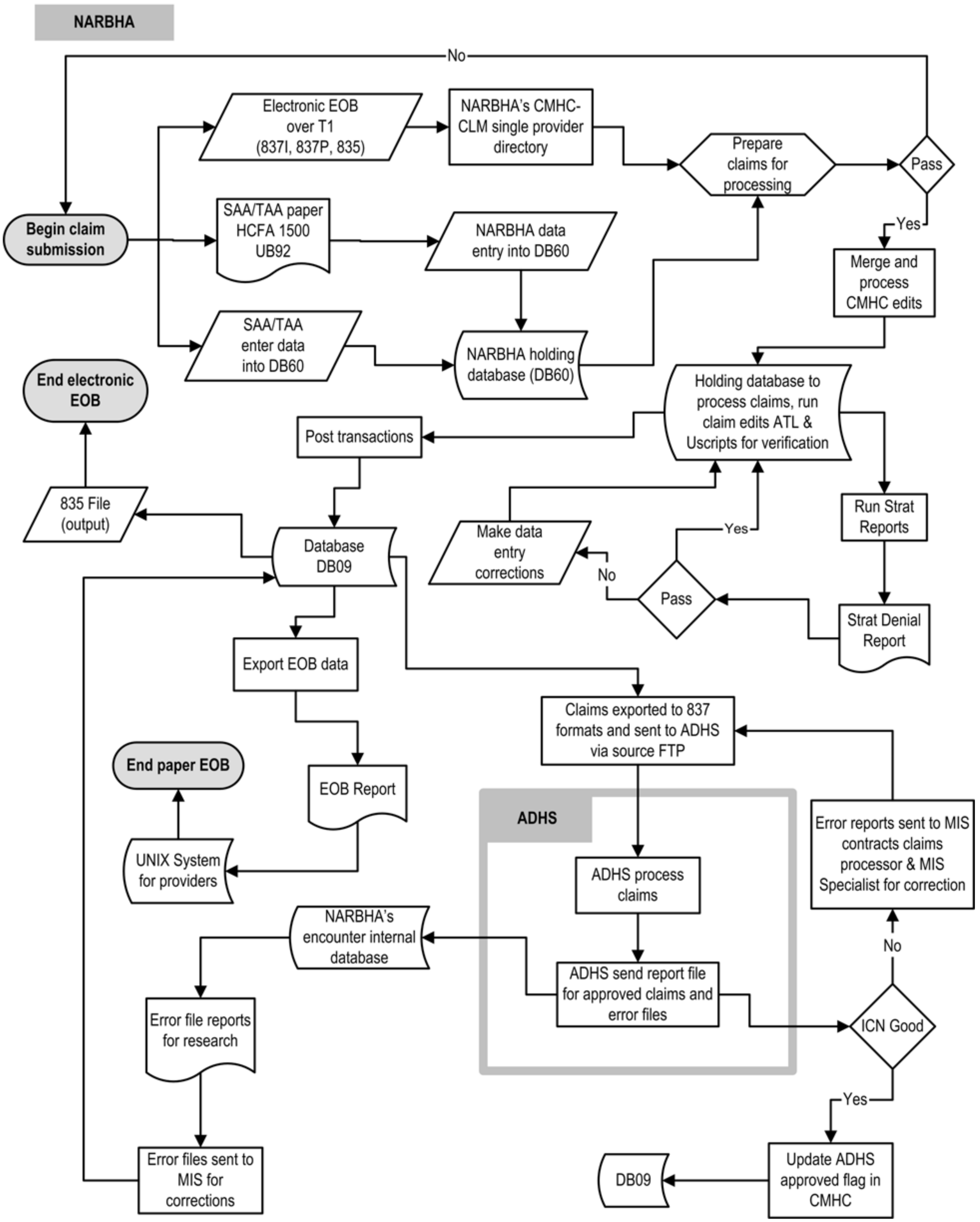
From DB09, claims are exported into a HIPAA 837 Professional or HIPAA 837 Institutional formats and are sent to ADHS/DBHS via a secure FTP connection. ADHS/DBHS processes claims nightly so NARBHA receives the files the next day.

Data Flow back to NARBHA

NARBHA receives two files back from ADHS. One file is the accepted production data. This information is then applied to a mirror database containing data that ADHS has posted as accepted claims/encounters. If errors occur while applying data, reports are sent to MIS for correction. Error files are processed in a program called ICNGOOD, which separates data based on error category, and are then sent to the proper NARBHA department for resolution. Once claims are corrected, they are resubmitted to ADHS/DBHS through the same process.

NARBHA's claim/encounters processing data flow is shown in Diagram 5.k.3.

Diagram 5.k.3 **Claims/Encounters Processing Data Flow**


NARBHA
No
Electronic EOB over T1 (837I, 837P, 835)
NARBHA's CMHC-CLM single provider directory
Prepare claims for processing
Pass
Yes
Begin claim submission
SAA/TAA paper HCFA 1500 UB92
NARBHA data entry into DB60
Merge and process CMHC edits
SAA/TAA enter data into DB60
NARBHA holding database (DB60)
End electronic EOB
Holding database to process claims, run claim edits ATL & Uscripts for verification
Post transactions
835 File (output)
Run Strat Reports
Yes
Make data entry corrections
Database DB09
No
Pass
Strat Denial Report
Export EOB data
Claims exported to 837 formats and sent to ADHS via source FTP
End paper EOB
EOB Report
ADHS
UNIX System for providers
ADHS process claims
Error reports sent to MIS contracts claims processor & MIS Specialist for correction
NARBHA's encounter internal database
No
ADHS send report file for approved claims and error files
Error file reports for research
ICN Good
Yes
Error files sent to MIS for corrections
DB09
Update ADHS approved flag in CMHC

1

National Council for Prescription Drug Programs Data Flow

The National Council for Prescription Drug Programs (NCPDP) is a not-for-profit organization consisting of members from virtually every sector of the pharmacy services industry. It has worked on pharmacy industry-specific standards, education programs, and legislative/regulator issues for over 25 years. The NCPDP Telecommunication Standard (version 5.1) was adopted as the standard for pharmacy claims under HIPAA and has been defined as the standard for submission of pharmacy claims data by NARBHA to ADHS/DBHS.

Data Interactivity between NARBHA and CaremarkPCS

NARBHA is currently contracted with CaremarkPCS for pharmacy benefits management services. CaremarkPCS has relationships with more than 700 pharmacies across Arizona and across the country. NARBHA maintains CaremarkPCS eligibility files with member level information through the submission of member eligibility records on a daily basis through secure data exchange processes using the CaremarkPCS secure (123 bit encryption) Internet system. NARBHA also has online access to the CaremarkPCS eligibility files for emergent enrollment, maintenance of prescriber-panel information, medication authorization, and prescription overrides as necessary to manage a member's medication benefit, thereby ensuring that NARBHA members obtain their medication in an efficient manner.

Data Flow from CaremarkPCS to NARBHA

The CaremarkPCS billing process is based on a two week cycle where CaremarkPCS submits invoices to NARBHA for payment of medication claims every two weeks, and submits the medication transaction level information to NARBHA 12 times per calendar year.

Data Flow at NARBHA

With the data received, NARBHA completes several discrete steps. These are:

- The medication transaction data file is retrieved from the CaremarkPCS systems through a secure data exchange process and imported into the NARBHA medication transaction reporting process. This file contains member-level data as to individual prescriptions filled, as well as file-summary-level data on record counts, total dollars, adjustments, administrative fees and so on.

- In-house programs review the various files for internal consistency and to balance detail level data to trailer summary totals. When these internal processes are complete, control reports are prepared for the NARBHA Finance Department to review and balance to the previously submitted CaremarkPCS invoices.
    - If there is no discrepancy between the reports, the NARBHA Finance Department authorizes NARBHA MIS to proceed with the next step.
    - If there is a discrepancy between the control reports and CaremarkPCS invoices, the NARBHA MIS and/or Finance Departments contact CaremarkPCS to resolve the issue. Resolution steps can include a re-run of the files at NARBHA, re-creation of the file at CaremarkPCS and retrieval of that new file to be re-run at NARBHA, or an authorization by the Finance department to accept the variance and reconcile it against subsequent months.

- With approval from the NARBHA Finance Department, MIS adds the transaction data to the NARBHA medication database.

Data Flow to ADHS/DBHS

MIS prepares the HIPAA-compliant NCPDP claim transactions that contain all current medication claims data, and any medication claims data that have been corrected from previous submission failures. The NCPDP is transmitted to ADHS/DBHS through a secure FTP process.

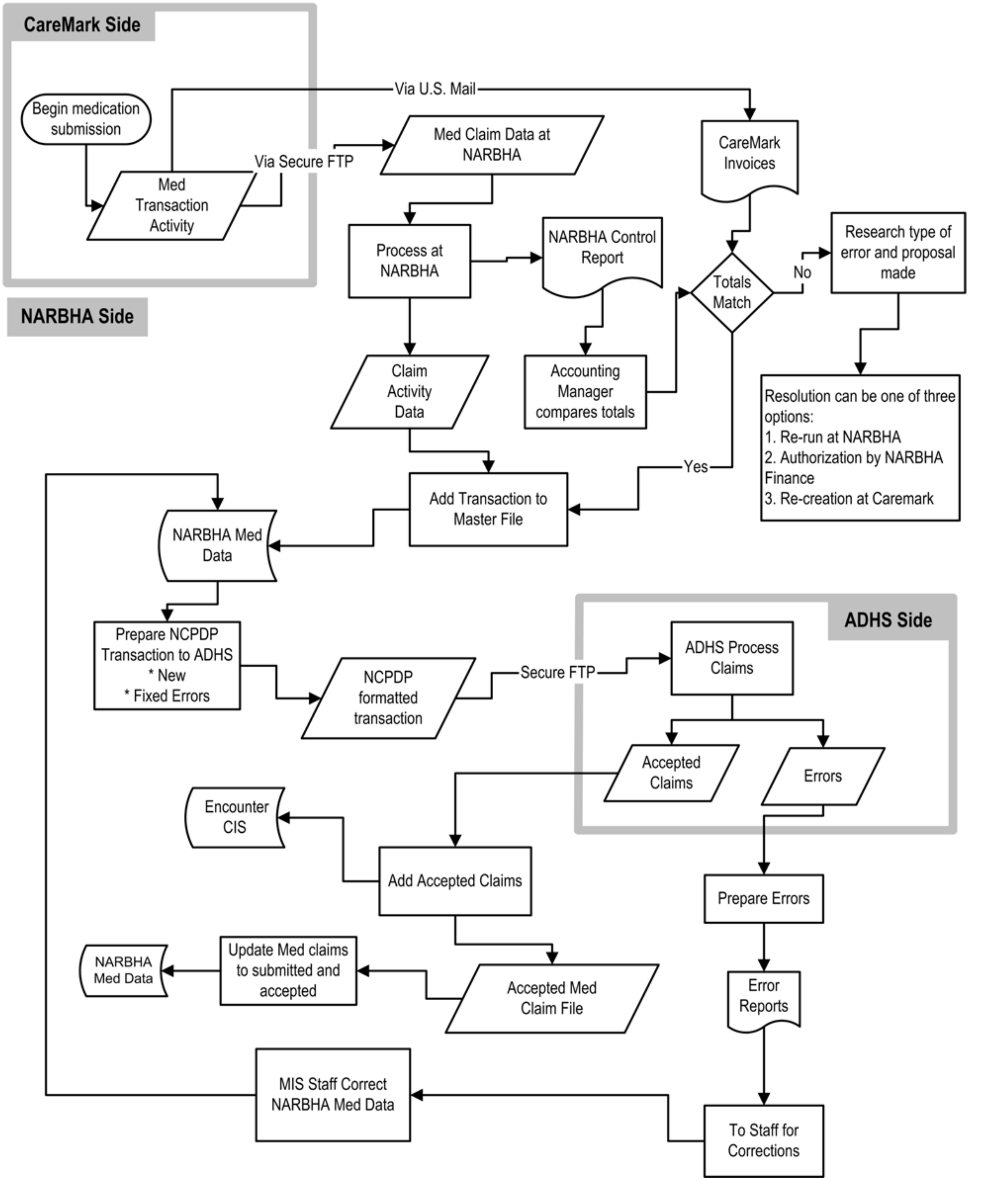
Data Flow back to NARBHA

After ADHS/DBHS has processed the NCPDP transactions, two files are returned to NARBHA. Accepted NCPDP claims are returned to NARBHA through the ADHS/DBHS claims download process and are added to the NARBHA internal file. Updates from this process are used to mark the medication claims in the NARBHA medication database as submitted and accepted. A separate file containing errors is returned to NARBHA. This file is used to generate error reports, which are distributed to appropriate staff for research and resolution. Corrections are submitted to MIS for correction in the NARBHA medication database. Corrected medication claims are then marked for re-submission to ADHS/DBHS.

Diagram 5.k.4 shows NARBHA's NCPDP data flow.

Diagram 5.k.4

NCPDP Data Flow



1

DATA CAPTURE AT NARBHA

Data Capture is defined as the electronic or hard-copy information that is submitted to NARBHA by its providers or ADHS/DBHS and is used by NARBHA to satisfy its contractual requirements or to manage its data systems effectively. The processes below address the data capture aspects of NARBHA's technical environment.

- Substance Abuse Prevention and Treatment (SAPT)
- Correctional Officer/Offender Liaison (COOL)
- AHCCCS Eligibility Application files
- ADHS/DBHS Withholding Files
- ADHS/DBHS Third Party Liability
- Institutions for Mental Disease
- Respite Tracking
- CPS 24-Hour Response

Substance Abuse Prevention and Treatment Process

Substance Abuse Prevention and Treatment (SAPT) is a federal grant program for individuals, including IV drug users or substance-abusing pregnant or parenting women, who qualify to receive substance abuse treatment. Only new enrollments are captured by NARBHA's system. NARBHA is responsible for monitoring these members and making sure they receive treatment in a timely fashion. NARBHA sends a report on qualifying individuals to the SAAs/TAAs, which are required to reconcile their records against NARBHA's report for verification.

Data Flow at the SAAs/TAAs

SAPT eligibility is determined by a set of federal requirements. These requirements have been distributed to all the SAAs/TAAs to enable their front desk and clinical staff to immediately recognize a SAPT-eligible member or referral.

Data Flow at NARBHA

NARBHA uses those same determinations in a program called SAPT, which uses data exported from the CMHC-MCO system. The export is run 20 days after the SAPT reporting time period ends, to ensure that all admits and initial demographic data to be submitted to NARBHA have been received. For example, NARBHA runs a report in late May on qualifying members for April.

Data Flow from NARBHA to the SAAs/TAAs

For all admits meeting the qualifications, NARBHA creates an electronic form, which is e-mailed to the SAAs/TAAs, filled out, and faxed back to NARBHA. This form requires SAAs/TAAs to enter in the type of services or referrals they rendered.

Data Flow to ADHS/DBHS

Once NARBHA receives the form, the responsible party at NARBHA enters the services or referrals into the SAPT database, generates reports, and sends them to ADHS/DBHS to show overall percentages of compliance.

Correctional Officer/Offender Liaison Process

Correctional Officer/Offender Liaison (COOL) members are individuals with a substance abuse problem who have recently been released from jail. The parole officer sends NARBHA a written referral with the location of the SAA/TAA site at which the parolee is required to appear for treatment. This information is added to the COOL database, which is a proprietary software package developed by NARBHA, and a copy of the referral is sent to the site along with a report indicating the date by which the parolee needs to have his or her assessment and first treatment.

Every month the person at NARBHA who is responsible for tracking COOL members generates a report from the COOL database for each current enrollee and sends it to the appropriate SAA/TAA site. The SAA/TAA site provides all attendance dates and no-shows, and then faxes the report back to NARBHA with reasons for missed appointments. The staff member then enters this information into the COOL database.

NARBHA reports the number of enrollees to ADHS/DBHS every quarter, and sends a Community Service End Date monthly to the SAA/TAA sites notifying them when paroles end for each enrollee, because COOL funds will not pay for treatment beyond that date. Enrollees can, however, pay for further treatment through other sources if they wish.

ADHS/DBHS AHCCCS Eligibility Application Files

ADHS/DBHS provides NARBHA with a series of Microsoft Access databases that reflect the status of AHCCCS eligibility applications submitted by the SAAs/TAAs on behalf of members that may be AHCCCS-eligible. The databases, once downloaded, are made available to the supervisor of the NARBHA Member Service Representatives (the Performance Improvement Manager), whose department parses this information into reports by agency that submitted the original eligibility application. These reports are distributed to allow those SAAs/TAAs to follow through on the process.

ADHS/DBHS Withholding Files

ADHS/DBHS provides NARBHA with a series of data files known as the "Withhold" files. The Withhold files represent the claim-level detail data that ADHS/DBHS uses in preparing their Encounter Withhold Calculation spreadsheets. The Withhold files are available on a monthly basis, on approximately the first week of each calendar month, and are on the ADHS/DBHS server in the area reserved for NARBHA specific data.

The Withhold claim-level data files are retrieved by internal NARBHA MIS processes, the data is added to a series of internal databases, and reports are prepared to compare against the ADHS/DBHS published Encounter Withhold Calculation spreadsheets. There are several additional uses for these files:

- Comparison of the Withhold claim-level data against NARBHA internal fund allocation system data to determine if there are possible discrepancies in the allocation process.
- Comparison of the Withhold claim-level data against NARBHA internal databases that mirror the ADHS/DBHS CIS encounter data to determine if there are possible discrepancies.
- Comparison of the Withhold claim-level data against NARBHA CMHC-MCO claim databases to reconcile claims submitted against claims accepted.

Third Party Liability

NARBHA uses a Third Party Liability (TPL) file from AHCCCS that gives NARBHA general information such as effective and lapse dates on Medicare Part A and Medicare Part B members. This file was initially given to NARBHA in its entirety and is now updated daily through changes provided by ADHS/DBHS and applied to the TPL file. NARBHA pulls these files from ADHS/DBHS during morning production and applies changes to the table. Twice a month MIS processes this file, extracts data from the table, and imports the data into the CMHC/MCO system. These data in CMHC/MCO are used for validation of claims/encounters with clients that have a third party payer.

Institutions for Mental Disease

Institutions for Mental Disease (IMD) are defined in 42 CFR 435.1009 as a hospital, nursing facility, or other institution of more than 16 beds that is primarily engaged in providing diagnosis, treatment, or care of persons with mental diseases, including medical attention, nursing care, and related services. The regulations indicate that an institution is an IMD if its overall character is that of a facility established and maintained primarily for the care and treatment of individuals with mental diseases. Title XIX of the Social Security Act provides that, except for individuals under age 21 receiving inpatient psychiatric care, Medicaid (Title XIX) does not cover services to IMD patients under 65 years of age [section 1905 (a)(24)(B)].

IMD tracking allows NARBHA to track and analyze members' use and service limitations. It keeps track of IMD member stays by fiscal year, including Admit and Discharge date to allow NARBHA to make good decisions pertaining to IMD limitations. NARBHA also can accurately report IMD utilization information to other RBHAs.

<u>IMD Data Flow</u>

NARBHA collects admit/discharge data from IMD providers daily using the defined IMD Admit/Discharge AHCCCS form. These forms are faxed daily to NARBHA for all new admits and/or updates to existing admits. The data are entered into the IMD tracker, an application created by MIS. Return reports are generated and sent to both the IMD provider and the SAA/TAA responsible for the member involved, providing consistent communication among agencies.

Reports also are available to identify members who are approaching their service limitations, members in a particular IMD, members currently in any IMD, or members with overlapping stays. NARBHA MIS also has set up processes for any state agency to inquire as to a member's current service use. In addition, NARBHA's Member Service Representatives have the ability to verify member usage.

ADHS/DBHS Respite Tracking

As noted in other volumes of this RFP, NARBHA has implemented processes to track and monitor utilization of respite services by enrolled members to ensure that individual Title XIX/Title XXI members do not use more than 720 hours of respite services in any contract year. This tracking utilization process is managed by staff in NARBHA's Quality Management Department on a weekly basis.

NARBHA MIS has implemented a series of claims adjudication edits that monitor the utilization of respite services by members and will deny any claim that is in excess of a member's allowed 720 hours of respite services per contract year.

CPS 24-Hour Response

NARBHA MIS has developed an application to track children who are removed from their homes by Child Protective Services (CPS) and are not returning within 48 to 72 hours. NARBHA is responsible for ensuring that its SAAs/TAAs perform routine follow-ups on the children and their foster families, and provide CPS case managers with information regarding the case within 10 days of removal.

NARBHA is mandated by ADHS/DBHS to ensure that its SAAs/TAAs identify a potential member's safety needs and presenting problems and provide direct support to each child making the transition into foster care. The purpose is to stabilize crises and to be able to offer the immediate services and support each child may need. It is NARBHA's responsibility to provide CPS case managers with findings and recommendations for the initial Preliminary Protective Hearing, related to placement, services, and visitation for each child.

NARBHA's 24-Hour CPS Tracker application is designed to track all information about children referred by CPS in order to help NARHBA and the SAAs/TAAs in:

- Implementing Governor Napolitano's recommendations for CPS reform, including immediate access to behavioral health assessment and services for children being removed
- Recognizing a more global perspective on the trauma of removal
- Recognizing the need for ongoing development of integrated child welfare and behavioral health efforts for children in both systems
- Supporting best-practice initiatives in line with the Arizona Vision and Children's Principles

<u>CPS 24-Hour Response Data Flow</u>

- CPS calls the dedicated ProtoCall 24-Hour Response 1-800 line to request a response.
- ProtoCall informs the appropriate SAA/TAA regarding the event and the SAA/TAA staff calls the CPS worker and gathers relevant information such as the outcome of the CPS Safety Assessment; the reason for removal; how, when, why, and where the removal occurred; any known special needs of the child; any known supports for the child; where siblings are; any known needs of the new caregiver; etc.
- Staff at the SAA/TAA contact the caregiver to schedule the face-to-face, in-placement response, to occur within 24 hours of referral.
- Out-of-home caregivers, behavioral health providers, and CPS communicate regarding the child's unique experience to develop an interim service plan that will address any immediate needs the child is experiencing and identify a point of contact for the caregiver in the behavioral health systems.

NARBHA's 24-Hour CPS Tracker collects data at each phase of this process, allowing NARBHA to accurately evaluate detailed information about the children in the program, such as age and eligibility, as well as identifying needs such as infant care.

<u>DATA ACCESS</u>

Data access is defined as facilitating NARBHA staff access to data systems supported by other, non-NARBHA, agencies that are necessary to allow NARBHA to perform specific functions as described within this RFP. NARBHA supports access to the following systems.

- ADHS/DBHS Office of Grievance and Appeal
- AHCCCS Prepaid Medical Management Information System (PMMIS)
- AHCCCS Online website

Office of Grievance and Appeal

NARBHA supports the programs/software necessary to allow NARBHA staff to access the ADHS/DBHS Office of Grievance and Appeals database. This application, written and supported by ADHS/DBHS technical staff, is used to record grievances, appeals, hearing dates, and other information as prescribed in the Office of Grievance and Appeals (OGA) Database Manual.

The NARBHA MIS Director or designee is responsible for procedures/policies to request, issue, monitor, and maintain User IDs for access to the CIS OGA databases. While the MIS Director or designee manages the process controlling access, the Grievance and Appeals Administrator at NARBHA is responsible for authorizing NARBHA staff to have access to the OGA databases.

AHCCCS PMMIS

NARBHA supports the software necessary to allow NARBHA staff to use the AHCCCS PMMIS system. The PMMIS application, written and supported by AHCCCS technical staff, is used by NARBHA staff to inquire into status of claims, member eligibility, and provider contract information.

The NARBHA MIS Director or designee is responsible for procedures and policies to request, issue, monitor, and maintain User IDs for access to the AHCCCS/PMMIS system. The MIS Director or designee manages the process controlling access and is responsible for authorizing NARBHA staff to have access to the AHCCCS/PMMIS system.

AHCCCS Online Website

NARBHA ensures that staff personal computers are configured so that authorized staff can use the web-based inquiry process, AHCCCS Online, that AHCCCS has made available to providers and RBHAs. The AHCCCS Online web applications, written and supported by AHCCCS technical staff, are used by NARBHA staff to inquire into status of claims and member eligibility.

The NARBHA MIS Director or designee is responsible for procedures and policies to request, issue, monitor, and maintain User IDs for access to the AHCCCS/PMMIS system. The MIS Director or designee manages the process controlling access and is responsible for setting up the master account and User ID and for issuing additional User IDs as necessary to provide NARBHA staff access to AHCCCS Online.

As the current Regional Behavioral Health Authority (RBHA) for Geographic Service Area 1 (GSA1), NARBHA satisfies all testing and data conversion requirements of ADHS/DBHS. NARBHA has consistently satisfied testing and data conversion requirements for ADHS/DBHS since December 1997; in fact, NARBHA was the first RBHA to be authorized to electronically capture client/claim data using internal systems, process claims adjudication, and submit that electronic data to AHDS/DBHS.

The last major conversion/testing processes between ADHS/DBHS and NARBHA were the implementation of the data transactions mandated by the Health Insurance Portability and Accountability Act (HIPAA) standards in August 2003 and the revisions required by ADHS/DBHS to implement the Demographic data transactions in October 2003. NARBHA was the second RBHA to accomplish these milestones; its participation allowed ADHS/DBHS to fully test the edits, ensuring a better product overall.

NARBHA is committed to and confident in its long history of data conversion, testing, and submission to ADHS/DBHS, and is fully prepared for any future requirements in this area.

Testing

When the contract for GSA1 has been finalized, NARBHA will immediately begin work with ADHS/DBHS to confirm and finalize the schedule proposed below for re-verification and testing of the data requirements laid out in this Request For Proposals (RFP) and the Client Information System (CIS) File Layout and Specifications Manual (ver 1.19 as included in this RFP). NARBHA's proposed schedule pre-supposes a start date of February 1, 2005. This plan will address:

- Testing of submission of required data files to ADHS/DBHS

- Testing of return submission of required data files to NARBHA

- Demonstration of access to the ADHS/DBHS CIS with procedures to monitor/maintain CIS User IDs issued to NARBHA staff

- Demonstration of access to the Arizona Health Care Cost Containment System (AHCCCS) Prepaid Medical Management Information Systems (PMMIS) with procedures to monitor/maintain User IDs issued to NARBHA staff

- Demonstration of access to the AHCCCS website with procedures to monitor/maintain User IDs issued to NARBHA staff

- Demonstration of access to the ADHS/DBHS Office of Grievance and Appeal (OGA) system with procedures to monitor/maintain UserIDs issued to NARBHA staff

- Demonstration of ability to access/download AHCCCS eligibility applications from ADHS/DBHS on the status of AHCCCS applications submitted to AHCCCS from the Department of Economic Security and the AHCCCS Central Screening Unit

- Certification that all transactions have been prepared by the appropriate data system and not manually manipulated/changed

- Demonstration that access to ADHS/DBHS CIS data systems for submission of electronic data is accomplished using encrypted technologies

The test/data conversion plan described below is based on the following assumptions:

- Technical staff at ADHS/DBHS are able to coordinate two tests per day, one in the morning and one in the afternoon.

- ADHS/DBHS staff are able to set up and identify a sufficient number of client IDs in their test system(s) to support a number of test transactions that is in excess of the daily test criteria.

- Members set up in the ADHS/DBHS test systems are/will be available for subsequent NARBHA testing processes. This will allow NARBHA to build the number of required test scenarios that will support the enrollment, closure, demographic, claims, and National Council Prescription Drug Programs (NCPDP) medication claim processes.

- ADHS/DBHS will have available a series of Statewide Rosters, AHCCCS Eligibility, and Third Party Liability files that reflect these test data.

- ADHS/DBHS staff will determine whether a fully functional test data set, unrelated to any production data set, is necessary or if a production data set from NARBHA can be used.

NARBHA test systems already are in existence and are used for testing of program and system changes. These systems consist of:

- A fully functional Managed Care Organization (MCO) data system within NARBHA's CMHC/MIS system, NARBHA's primary business application, which is used to track member level information. This test system can be configured to reflect the entire NARBHA production MCO system (for volume tests), or a portion of the MCO data system based on the scenarios to be tested.

- A fully functional Claims (CLM) data system within NARBHA's CMHC/MIS system. Again, this test system can be configured to reflect the entire NARBHA production CLM system (for volume tests), or a portion of the CLM data system based on the scenarios to be tested.

- A full 60 gigabytes of mass storage on the Novell network side to support the test environment, which is used to develop and test all Microsoft Visual FoxPro applications developed by NARBHA's Management Information Systems Department (MIS). The data sets for this test environment can be set to reflect the entire NARBHA non-CMHC file base (for volume tests), or just a portion of the non-CMHC file base based on the scenarios to be tested.

NARBHA MIS typically performs testing in parallel with current production systems, using production/real time data whenever possible. This allows the MIS department analyst to compare the results of the original/production process to the modified test systems results to see if the modifications were successful. If the test results do not meet expectations, the MIS analyst has the test and production data sets available that allow him/her to research why the test failed, resolve the problem, and re-test the process.

The NARBHA Test/Data Conversion Plan is on the following pages.

NARBHA Test/Data Conversion Plan

Step	Task	Description	Start Date	End Date	Outcomes	Comments
1		**Review RFP and CIS manual for requirements**	2/1/2005	2/18/2005		
	1.1	834 Enrollment/Intake	2/1/2005	2/18/2005		
	1.2	Demographic	2/1/2005	2/18/2005		
	1.3	837 Institutional/UB92	2/1/2005	2/18/2005		
	1.4	837 Professional/HCFA	2/1/2005	2/18/2005		
	1.5	Medication Claim/NCPDP	2/1/2005	2/18/2005		
	1.6	Miscellaneous Files	2/1/2005	2/18/2005		
	1.7	System(s) access	2/1/2005	2/18/2005		
	1.8	Set up test systems (ADHS/NARBHA)	2/1/2005	2/18/2005		
2		**834/Enrollment**	2/21/2005	3/4/2005		
	2.1	Set test data criteria consistent with ADHS/DBHS test system	2/21/2005	3/4/2005		Set test file totals/limits
	2.2	Create data/modify production data	2/21/2005	3/4/2005		
	2.3	Submit 834/Intake (Add/Change)	2/21/2005	3/4/2005		90+% acceptance
	2.4	Accept return 834/Intake (Dintd) information and process at NARBHA	2/21/2005	3/4/2005		
	2.5	Repeat 2.1 - 2.4 for 834/Closures	2/21/2005	3/4/2005		Volumes set at 100% of adds and 90+% acceptance
	2.6	Complete process successfully	2/21/2005	3/4/2005		Acceptance letter detailing successful test(s). Incremental letters appropriate
3		**Demographic**	3/7/2005	3/18/2005		
	3.1	Set test data criteria consistent with ADHS/DBHS test system	3/7/2005	3/18/2005		Set test file totals/limits
	3.2	Create data/modify production data	3/7/2005	3/18/2005		
	3.3	Submit Demographic File Layout	3/7/2005	3/18/2005		90+% acceptance
	3.4	Accept return Demographic information and process at NARBHA	3/7/2005	3/18/2005		
	3.5	Repeat 3.1 - 3.4 for Initial submission	3/7/2005	3/18/2005		Volumes set at 100% of adds and 90+% acceptance

Step	**Task**	**Description**	**Start Date**	**End Date**	**Outcomes**	**Comments**
	3.6	Repeat 3.1 - 3.4 for Update submission	3/7/2005	3/18/2005		Volumes set at 35% of adds and 90+% acceptance
	3.7	Repeat 3.1 - 3.4 for Annual submission	3/7/2005	3/18/2005		Volumes set at 100% of adds and 90+% acceptance
	3.8	Repeat 3.1 - 3.4 for Disenrollent submission	3/7/2005	3/18/2005		Volumes set at 100% of adds and 90+% acceptance
	3.9	Complete process successfully	3/7/2005	3/18/2005		Acceptance letter detailing successful test(s). Incremental letters appropriate
4		**837 Institutional/UB92**				
	4.1	Set test data criteria consistent with ADHS/DBHS test system	3/7/2005	3/18/2005		Set test file totals/limits
	4.2	Create data/modify production data	3/7/2005	3/18/2005		
	4.3	Submit HHIPAA/837I (UB92) file	3/7/2005	3/18/2005		90+% acceptance
	4.4	Accept return Claim data (DENCD) information and process at NARBHA	3/7/2005	3/18/2005		
	4.5	Repeat steps 4.1 through 4.3 for Void transactions	3/7/2005	3/18/2005		Volumes set at 10% of adds and 90+% acceptance
	4.6	Complete process successfully	3/7/2005	3/18/2005		
5		**837 Professional/HCFA**				
	5.1	Set test data criteria consistent with ADHS/DBHS test system	3/21/2005	4/1/2005		Set test file totals/limits
	5.2	Create data/modify production data	3/21/2005	4/1/2005		
	5.3	Submit HHIPAA/837P (HCFA) file	3/21/2005	4/1/2005		90+% acceptance
	5.4	Accept return Claim data (DENCD) information and process at NARBHA	3/21/2005	4/1/2005		
	5.5	Repeat steps 5.1 through 5.3 for Void transactions	3/21/2005	4/01/2005		Volumes set at 10% of adds and 90+% acceptance
	5.6	Complete process successfully	3/21/2005	4/1/2005		

1

1

6		**Medication Claim/NCPDP**				
	6.1	Set test data criteria consistent with ADHS/DBHS test system	3/21/2005	4/1/2005		Set test file totals/limits. Insure that 25% have companion data
	6.2	Create data/modify production data	3/21/2005	4/1/2005		
	6.3	Submit HHIPAA/837P (HCFA) file	3/21/2005	4/1/2005		90+% acceptance
	6.4	Accept return Claim data (DENCD) information and process at NARBHA	3/21/2005	4/1/2005		
	6.5	Complete process successfully	3/21/2005	4/1/2005		
7		**Miscellaneous**				
	7.1	Demonstrate compliance with Statewide Roster file download	4/4/2005	4/6/2005		
	7.2	Demonstrate compliance with Third Party Liability file download	4/4/2005	4/6/2004		
	7.3	Demonstrate compliance with AHCCCS Eligibility download	4/7/2005	4/11/2005		
	7.4	Demonstrate compliance with RBHA Withhold file download	4/7/2005	4/11/2005		
	7.5	Demonstrate compliance with Provider/Reference file (AHCCCS) download	4/12/2005	4/15/2005		
	7.6	Demonstrate compliance with AHCCCS eligibility application file download	4/12/2005	4/15/2005		
	7.7	Complete process successfully	4/4/2005	4/15/2005		Acceptance letter detailing successful test(s). Incremental letters.
8		**System(s) access**				
	8.1	Procedures to request, monitor, terminate access	4/4/2005	4/8/2005		
	8.2	Online access to ADHS/DBHS system - Client Information System	4/4/2005	4/8/2005		
	8.3	Online access to ADHS/DBHS system - Office of Grievance and Appeal	4/4/2005	4/8/2005		

	8.4	Online access to AHCCCS/PMMIS for eligibility determination	4/4/2005	4/8/2005		
	8.5	Online access to AHCCCS Online for eligibility determination	4/4/2005	4/8/2005		
	8.6	Complete process successfully	4/4/2005	4/8/2005		Acceptance letter detailing successful test(s). Incremental letters.
9		**Final Compliance review**				
	9.1	Review	4/18/2005	4/18/2005		Final Acceptance/compliance letter issued

1

System/File Change Notification
Upon approval of these data file interfaces by ADHS/DBHS, during the data/conversion verification phase NARBHA will preserve the systems, programs, and/or specifications as approved during the process. NARBHA will, when necessary, make changes to these systems, programs, and/or specifications that are necessary to support its business model.

If these changes are deemed to be major, defined as systems changes at a level that would require re-testing and re-certification by ADHS/DBHS as to the acceptability of the data, NARBHA will notify ADHS/DBHS, in writing or by e-mail as to the change. NARBHA will notify both the ADHS/DBHS Information Technology Services Project Lead and the Office of Program Support and will include the nature of the change(s) and testing plan(s) in place at NARHBA to test the process and re-verify the data, and, if necessary, will request that ADHS/DBHS participate in the data conversion/testing process.

Systems Access Change Notification
Upon approval of the Systems Access testing/verification process (Step 8 above) proving that NARBHA personal computers can access the ADHS/CIS system, the DBHS/OHR system, the DBHS/OGA system, and the AHCCCS/PMMIS system, NARBHA will ensure that configuration(s) necessary for the personal computers to access these systems remain unchanged. NARBHA will continue, as necessary, to provide technology upgrades, hardware, and software, as the technology matures and NARBHA needs indicate an upgrade is necessary. Prior to any technology rollout for personal computers used to access these systems, NARBHA will test the technology, show it to allow the same level of functionality, and notify ADHS/DBHS as to the upgrade.

Overall
NARBHA has a longstanding commitment to the testing and data conversion process and has built excellent working relationships with ADHS/DBHS staff in this area. Staffing patterns in NARBHA MIS reflect this commitment. The mix of employees includes:

- A Programming unit with six staff positions (one currently vacant). Current staff have a mix of skills totaling 37 years experience in the MIS technical area and totaling 32 years experience in the behavioral health industry. MIS staff have primary experience in the uses of CMHC/MIS as the business application package, Microsoft Visual FoxPro for network-based applications, and Visual Studio .Net for web applications.
- A Wide Area Network/Local Area Network (LAN/WAN) unit consisting of a manager and two staff with a total of 24 years experience in this area. A number of support contracts in this area provide additional backup.
- A Production/Operations unit consisting of a manager and three MIS specialists with a total of 15 years experience at the RBHA and provider levels to support the operational aspects of the NARBHA system including error identification, research, and correction.

NARBHA realizes that only through a collaborative design, testing, and implementation process with ADHS/DBHS that includes strong automation components and operational procedures can the best information be gathered to serve the needs of ADHS/DBHS, NARBHA, and members.